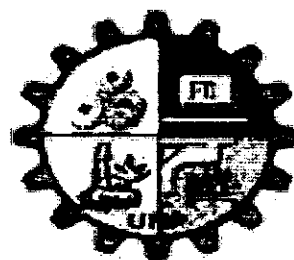


**UNIVERSIDAD NACIONAL DE PIURA**

**FACULTAD DE INGENIERIA INDUSTRIAL  
ESCUELA PROFESIONAL DE INGENIERIA  
INFORMATICA**



**TESIS**

**PROPUESTA DE UN PLAN DE AUDITORIA INFORMATICA PARA  
EL “SISTEMA DE INFORMACION EN SALUD” Y EL  
“APLICATIVO PARA EL REGISTRO DE FORMATOS SIS” EN LOS  
ESTABLECIMIENTOS DE SALUD DE LA UNIDAD EJECUTORA  
400 EN LA REGION PIURA EN EL AÑO 2015**

**PRESENTADA POR:**

**CARMEN CYNTHIA ELIZABETH RAMOS ARCA**

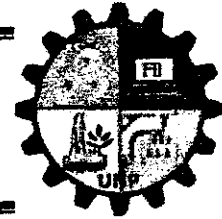
**TESIS PARA OPTAR EL TITULO DE  
INGENIERO INFORMATICO**

**PIURA, PERU  
JUNIO 2015**

500  
RAM



**UNIVERSIDAD NACIONAL DE PIURA  
FACULTAD DE INGENIERÍA INDUSTRIAL  
DECANATO**



**ACTA DE SUSTENTACIÓN DE TESIS**

Los Miembros del Jurado Calificador Ad-Hoc de la Tesis denominada:  
**«PROPUESTA DE UN PLAN DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA DE INFORMACIÓN EN SALUD Y EL APLICATIVO PARA EL REGISTRO DE FORMATOS SIS EN LOS ESTABLECIMIENTOS DE SALUD DE LA UNIDAD EJECUTORA 400 EN LA REGIÓN PIURA DEL AÑO 2015»**,  
presentada por la señorita **CARMEN CYNTHIA ELIZABETH RAMOS ARCA**,  
Bachiller de la Escuela Profesional en Ingeniería Informática; asesorada por el  
**Ing. Néstor Manuel Castillo Burgos, MSc. y co asesorada por el Ing. Persi Williansh Cabrera Antón, MBA.**; reunidos para la sustentación de ésta y  
luego de escuchar su exposición y las respuestas a las preguntas formuladas,  
la declaran:

**APROBADO**


**Con el Calificativo:**

**MUY BUENO**



En consecuencia la sustentante se encuentra apta para recibir el título profesional de **INGENIERO INFORMÁTICO**, conforme a Ley.

Piura, 20 de junio del 2015

  
**Ing. FRANCISCO JAVIER CRUZ VILCHEZ, MSc.**  
**PRESIDENTE - JURADO CALIFICADOR**

  
**Ing. PERDO ANTONIO CRUJLO GONZALES, MSc.**  
**VOCAL - JURADO CALIFICADOR**

  
**Ing. HÉCTOR WILMER FIESTAS BANCAYÁN, MSc.**  
**SECRETARIO - JURADO CALIFICADOR**

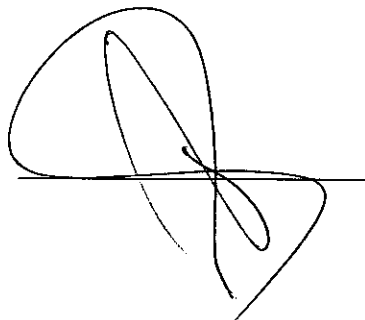
Tesis presentada como requisito para optar el título de Ingeniero Informático

ASESOR:



Ing. Néstor Manuel Castillo Burgos

CO – ASESOR:



Ing. Persi Williansh Cabrera Antón

TESISTA:



Carmen Cynthia Elizabeth Ramos Arca

## **DEDICATORIA**

Esta tesis está dedicada muy especialmente a mi familia, quienes me han sabido apoyar incondicionalmente para la culminación de mi carrera profesional. A todas las personas que me han ayudado a ser mejor persona y profesional en el proceso de mi vida.

## **AGRADECIMIENTO**

A Dios por brindarme salud y la capacidad para cumplir una de mis metas en la vida. De manera muy especial a mi mamá por la confianza y el apoyo que me ha otorgado en todo momento. A las personas que me han extendido su mano cuando yo los necesitaba. Al jefe de estadística e informática por brindarme la ayuda e información necesaria para culminar mi tesis. A mi asesor por el apoyo en las revisiones graduales de mi tesis.

## **RESUMEN**

El presente trabajo de tesis tiene como objetivo principal proponer un plan de auditoría informática para los dos sistemas más importantes de cada establecimiento de salud, los cuales son el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.

Para alcanzar dicho objetivo, se ha planteado los siguientes objetivos específicos:

- Conocer la organización, normas y procedimientos de la Unidad Ejecutora 400 de la Región Piura donde para el cual se realizará la propuesta del Plan de Auditoría.
- Establecer los objetivos de control y los procedimientos de auditoría a aplicar sobre el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.
- Determinar el programa de auditoría que se utilizará de guía para ejecutar el Plan de Auditoría.

Al respecto, la propuesta del plan de auditoría informática se ha realizado en base a la Guía de Control Interno de las entidades del Estado Peruano para realizar un análisis de riesgos de ambos sistemas de información basadas en encuestas aplicadas a 10 establecimientos de salud, además se aplicó la Norma Técnica Peruana ISO 27001: 2008 con la finalidad de establecer los objetivos y procedimientos de control adaptados a los establecimientos de salud para posteriormente plasmarlo en el programa detallado de auditoría informática y aplicarlo en un futuro mediante el papel de trabajo por cada procedimiento de control.

Todo esto con la finalidad de brindar una guía para las futuras auditorías a los sistemas informáticos del estado peruano, tomando como base la propuesta del plan de auditoría informática y a la vez facilitando la identificación de los riesgos existentes asociados a los controles de los procesos informáticos que acarrea cada sistema, los cuales pueden afectar el logro de los objetivos y metas de cada institución.

## **ABSTRACT**

This thesis has as main objective to propose a plan of audit information for the two most important systems of each health, which are the Health Information System and application to record Format SIS.

To achieve this objective, it has set the following objectives:

- Understand the organization, rules and procedures of the execution unit 400 of the Piura region where for which the proposed Audit Plan will be made
- Establishing control objectives and audit procedures to be applied to the Health Information System and application to record Format SIS.
- Determining the audit program to be used as a guide for executing the audit plan.

In this regard , the proposal of computer audit plan has been carried out based on the Guide to Internal Control of Peruvian government entities to conduct a risk analysis of both information systems based on surveys applied to 10 health facilities , further applied the International Standard ISO 27001 : 2008 in order to establish the objectives and control procedures adapted to health facilities and later translate it into detailed computer program audit and apply it in the future through the paper work for each procedure control.

All this in order to provide guidance for future audits to computer systems of the Peruvian state , based on the proposal of computer audit plan and also facilitating the identification of the risks associated with computer controls processes carries each system , which may affect the achievement of the objectives and goals of each institution.

# INDICE

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>CAPITULO 1: EL PROBLEMA DE INVESTIGACIÓN</b>             | <b>2</b> |
| 1.1      | Descripción del problema                                    | 2        |
| 1.2      | Formulación del problema                                    | 4        |
| 1.3      | Objetivos de la investigación                               | 4        |
| 1.3.1    | Objetivo General  | 4        |
| 1.3.2    | Objetivos específicos                                       | 4        |
| 1.4      | Justificación, importancia y beneficios de la investigación | 5        |
| 1.4.1    | Justificación   | 5        |
| 1.4.2    | Importancia   | 5        |
| 1.4.3    | Beneficiarios de la Investigación                           | 5        |
| 1.5      | Hipótesis   | 6        |
| 1.5.1    | Hipótesis principal   | 6        |
| 1.5.1.1  | Identificación y operacionalización de las variables        | 6        |
| <b>2</b> | <b>CAPITULO 2: MARCO TEÓRICO</b>                            | <b>8</b> |
| 2.1      | Antecedentes  | 8        |
| 2.2      | Actividad empresarial                                       | 9        |
| 2.2.1    | Dirección Regional de Salud – Piura                         | 9        |
| 2.2.1.1  | Reseña Histórica  | 9        |
| 2.2.1.2  | Misión  | 9        |
| 2.2.1.3  | Visión  | 9        |
| 2.2.1.4  | Funciones   | 10       |
| 2.2.1.5  | Ámbito de ejecución   | 10       |
| 2.2.1.6  | Unidad Ejecutora 400  | 11       |
| 2.2.2    | Seguro Integral de Salud                                    | 12       |
| 2.2.2.1  | Misión  | 12       |
| 2.2.2.2  | Visión  | 12       |
| 2.2.2.3  | Valores Institucionales                                     | 13       |
| 2.2.2.4  | Objetivos   | 13       |
| 2.2.3    | Base legal de la Unidad Ejecutora 400                       | 14       |
| 2.2.4    | Resolución Jefatural N° 170 – 2012 / Sis                    | 15       |
| 2.2.4.1  | Alcance   | 15       |
| 2.2.4.2  | Finalidad   | 15       |



|         |  |    |
|---------|--|----|
| 2.2.4.3 | Objeto.....  | 15 |
| 2.2.4.4 | PCPP: Proceso de Control Presencial Posterior de las prestaciones de Salud ..                                | 15 |
| 2.2.4.5 | Auditoria ejecutada .....  | 16 |
| 2.3     | Bases teóricas .....   | 16 |
| 2.3.1   | Auditoria en sistemas de información .....   | 16 |
| 2.3.1.1 | Auditoria.....   | 16 |
| 2.3.1.2 | Tipos de Auditorias .....  | 17 |
| 2.3.1.3 | Auditoria Informática .....  | 18 |
| 2.3.2   | Sistemas de control.....   | 19 |
| 2.3.2.1 | Control interno .....  | 19 |
| 2.3.2.2 | Control externo.....   | 19 |
| 2.3.3   | Evaluación de riesgos.....   | 20 |
| 2.3.4   | Seguridad de la Información .....  | 21 |
| 2.3.5   | Amenazas y vulnerabilidades .....  | 22 |
| 2.3.5.1 | Amenazas .....   | 22 |
| 2.3.5.2 | Vulnerabilidades.....  | 22 |
| 2.3.6   | Sistemas de información .....  | 23 |
| 2.3.7   | Plan de auditoria informática .....  | 24 |
| 2.3.7.1 | Objetivo de Control .....  | 24 |
| 2.3.7.2 | Procedimiento de Auditoria.....  | 25 |
| 2.4     | Normatividad.....  | 26 |
| 2.4.1   | LEY N° 27785: Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la Republica. .... | 26 |
| 2.4.1.1 | Ámbito de aplicación .....   | 26 |
| 2.4.1.2 | Acción de control .....  | 27 |
| 2.4.2   | MAGU: Manual De Auditoria Gubernamental.....   | 27 |
| 2.4.2.1 | Concepto.....  | 27 |
| 2.4.2.2 | Objetivos .....  | 27 |
| 2.4.2.3 | Alcance.....   | 28 |
| 2.4.3   | NAGU .....   | 29 |
| 2.4.3.1 | Concepto.....  | 29 |
| 2.4.3.2 | Programas de auditoria.....  | 30 |
| 2.4.3.3 | Archivo permanente .....   | 31 |
| 2.4.3.4 | Estudio y evaluación de control interno .....  | 31 |

|         |   |           |
|---------|---|-----------|
| 2.4.4   | NTP ISO/IEC 27001:2008 .....  | 34        |
| 2.4.4.1 | Concepto.....   | 34        |
| 2.4.4.2 | Sistema de seguridad de la información .....                                    | 35        |
| 2.4.5   | Guía de control interno para el sector publico.....                             | 36        |
| 2.4.5.1 | Concepto.....   | 36        |
| 2.4.5.2 | Objetivos .....   | 36        |
| 2.4.5.3 | Ámbito de aplicación .....  | 36        |
| 2.4.5.4 | Clasificación del riesgo .....  | 38        |
| 2.4.5.5 | Valoración de los riesgos .....   | 39        |
| 2.4.5.6 | Matriz de probabilidad e impacto.....   | 40        |
| 2.4.5.7 | Riesgo residual .....   | 42        |
| 3       | <b>CAPÍTULO 3: DIAGNOSTICO SITUACIONAL DE LOS SISTEMAS DE INFORMACIÓN .....</b> | <b>43</b> |
| 3.1     | <b>Descripción del Sistema de Información en Salud.....</b>                     | <b>43</b> |
| 3.1.1   | Descripción General.....  | 43        |
| 3.1.2   | Características Técnicas .....  | 44        |
| 3.1.3   | Descripción de los procesos más importantes .....                               | 44        |
| 3.1.3.1 | Proceso de ingreso de datos.....  | 44        |
| 3.1.3.2 | Proceso de Edición de datos .....   | 45        |
| 3.1.3.3 | Proceso de envío de información .....   | 45        |
| 3.1.3.4 | Proceso de recepción de información por lotes .....                             | 46        |
| 3.1.3.5 | Proceso de creación de clave de digitador.....                                  | 47        |
| 3.1.3.6 | Proceso de mantenimiento de Personal .....                                      | 47        |
| 3.2     | <b>Descripción del Aplicativo para el Registro de Formatos SIS .....</b>        | <b>48</b> |
| 3.2.1   | Descripción General.....  | 48        |
| 3.2.2   | Características Técnicas .....  | 49        |
| 3.2.3   | Descripción de los procesos .....   | 49        |
| 3.2.3.1 | Acceso al aplicativo .....  | 49        |
| 3.2.3.2 | Registro de Formatos Únicos de Atención.....                                    | 50        |
| 3.2.3.3 | Reportes del aplicativo .....   | 51        |
| 3.2.3.4 | Backup de base de datos.....  | 52        |
| 3.2.3.5 | Restaurar base de datos .....   | 52        |
| 3.2.3.6 | Envío de información .....  | 53        |
| 3.2.3.7 | Cierre de periodo .....   | 53        |

|         |  |    |
|---------|--|----|
| 3.2.3.8 | Configuración del aplicativo .....   | 54 |
| 3.3     | Evaluación de riesgos.....   | 55 |
| 3.3.1   | Identificación de riesgos.....   | 55 |
| 3.3.1.1 | Técnica de recopilación de información .....   | 55 |
| 3.3.1.2 | Técnica de diagramación.....   | 57 |
| 3.3.1.3 | Registro de riesgo.....  | 58 |
| 3.3.2   | Valoración de riesgos .....  | 61 |
| 3.3.3   | Matriz de riesgos .....  | 62 |
| 3.3.4   | Matriz de situación de riesgo residual.....  | 66 |
| 4       | CAPÍTULO 4: PROPUESTA DE UN PLAN DE AUDITORIA INFORMÁTICA ...                                      | 67 |
| 4.1     | Alcance de la propuesta del plan de auditoría informática.....                                     | 67 |
| 4.2     | Criterios a aplicar de la propuesta del plan de auditoría informática .....                        | 67 |
| 4.3     | Definición de objetivos de control .....   | 67 |
| 4.3.1   | Objetivos de control para la evaluación de la Seguridad en Recursos Humanos .....                  | 67 |
| 4.3.2   | Objetivos de control para la evaluación de la seguridad física .....                               | 68 |
| 4.3.3   | Objetivos de control para la evaluación de la gestión de comunicaciones y operaciones.....         | 68 |
| 4.3.4   | Objetivos de control para la evaluación del control de accesos a los sistemas de información ..... | 68 |
| 4.3.5   | Objetivos de control para la gestión de incidentes en la seguridad de la información               | 69 |
| 4.3.6   | Objetivos de control para la evaluación de cumplimiento de normas .....                            | 69 |
| 4.3.7   | Objetivos de control para la evaluación de base de datos, archivos y datos .....                   | 69 |
| 4.4     | Procedimientos de Auditoria .....  | 69 |
| 4.5     | Programa de auditoria a aplicar.....   | 75 |
| 4.6     | Papeles de trabajo a aplicar .....   | 85 |
| 4.6.1   | Papel de trabajo 01: .....   | 85 |
| 4.6.1.1 | Formato para el recojo de evidencias .....   | 86 |
| 4.6.2   | Papel de trabajo 02 .....  | 87 |
| 4.6.2.1 | Formato para el recojo de evidencias .....   | 88 |
| 4.6.3   | Papel de trabajo 03 .....  | 89 |
| 4.6.3.1 | Formatos para el recojo de evidencias .....  | 90 |
| 4.6.4   | Papel de trabajo 04 .....  | 92 |
| 4.6.4.1 | Formatos para el recojo de evidencias .....  | 93 |
| 4.6.5   | Papel de trabajo 05 .....  | 94 |

|          |   |     |
|----------|---|-----|
| 4.6.5.1  | Formatos para el recojo de evidencias ..... | 95  |
| 4.6.6    | Papel de trabajo 06 .....                   | 97  |
| 4.6.6.1  | Formato para el recojo de evidencias .....  | 98  |
| 4.6.7    | Papel de Trabajo 07 .....                   | 99  |
| 4.6.7.1  | Formato para recojo de evidencias .....     | 100 |
| 4.6.8    | Papel de Trabajo 08 .....                   | 101 |
| 4.6.8.1  | Formatos para el recojo de evidencias ..... | 102 |
| 4.6.9    | Papel de trabajo 09 .....                   | 103 |
| 4.6.9.1  | Formatos para el recojo de evidencias ..... | 104 |
| 4.6.10   | Papel de trabajo 10 .....                   | 105 |
| 4.6.10.1 | Formatos para el recojo de evidencias ..... | 106 |
| 4.6.11   | Papel de trabajo 11 .....                   | 106 |
| 4.6.11.1 | Formatos para el recojo de evidencias ..... | 107 |
| 4.6.12   | Papel de trabajo 12 .....                   | 108 |
| 4.6.12.1 | Formato para el recojo de evidencias .....  | 109 |
| 4.6.13   | Papel de trabajo 13 .....                   | 110 |
| 4.6.13.1 | Formatos para el recojo de evidencias ..... | 111 |
| 4.6.14   | Papel de trabajo 14 .....                   | 112 |
| 4.6.14.1 | Formatos para el recojo de evidencias ..... | 113 |
| 4.6.15   | Papel de trabajo 15 .....                   | 114 |
| 4.6.15.1 | Formatos para el recojo de evidencias ..... | 115 |
| 4.6.16   | Papel de trabajo 16 .....                   | 116 |
| 4.6.16.1 | Formatos para el recojo de evidencias ..... | 117 |
| 4.6.17   | Papel de trabajo 17 .....                   | 118 |
| 4.6.17.1 | Formatos para el recojo de evidencias ..... | 119 |
| 4.6.18   | Papel de trabajo 18 .....                   | 120 |
| 4.6.18.1 | Formatos de recojo de evidencias .....      | 121 |
| 4.6.19   | Papel de trabajo 19 .....                   | 122 |
| 4.6.19.1 | Formatos de recojo de evidencias .....      | 123 |
| 4.6.20   | Papel de trabajo 20 .....                   | 124 |
| 4.6.20.1 | Formatos para el recojo de evidencias ..... | 125 |
| 4.6.21   | Papel de trabajo 21 .....                   | 126 |
| 4.6.21.1 | Formatos par el recojo de evidencias .....  | 127 |
| 4.6.22   | Papel de trabajo 22 .....                   | 128 |

|          |   |     |
|----------|---|-----|
| 4.6.22.1 | Formatos par el recojo de evidencias .....                                | 129 |
| 4.6.23   | Papel de trabajo 23 .....   | 130 |
| 4.6.23.1 | Formatos para el recojo de evidencias.....                                | 131 |
| 4.6.24   | Papel de trabajo 24 .....   | 132 |
| 4.6.24.1 | Formatos para el recojo de evidencias.....                                | 133 |
| 4.6.25   | Papel de trabajo 25 .....   | 134 |
| 4.6.25.1 | Formatos para el recojo de evidencias.....                                | 135 |
| 4.6.26   | Papel de trabajo 26 .....   | 136 |
| 4.6.26.1 | Formatos para el recojo de evidencias.....                                | 137 |
| 4.6.27   | Papel de trabajo 27 .....   | 138 |
| 4.6.27.1 | Formato para el recojo de evidencia.....                                  | 139 |
| 4.6.28   | Papel de trabajo 28 .....   | 140 |
| 4.6.28.1 | Formato de recojo de evidencias .....                                     | 141 |
| 4.6.29   | Papel de trabajo 29 .....   | 142 |
| 4.6.29.1 | Formato para el recojo de evidencias .....                                | 143 |
| 4.6.30   | Papel de trabajo 30 .....   | 144 |
| 4.6.30.1 | Formatos para el recojo de evidencias.....                                | 145 |
| 4.6.31   | Papel de trabajo 31 .....   | 146 |
| 4.6.31.1 | Formatos para el recojo de evidencias.....                                | 147 |
| 4.6.32   | Papel de trabajo 32 .....   | 148 |
| 4.6.32.1 | Formatos para el recojo de evidencias.....                                | 149 |
| 4.6.33   | Papel de trabajo 33 .....   | 150 |
| 4.6.33.1 | Formatos para el recojo de evidencias.....                                | 151 |
| 4.6.34   | Papel de trabajo 34 .....   | 152 |
| 4.6.34.1 | Formatos para el recojo de evidencias.....                                | 153 |
| 4.6.35   | Papel de trabajo 35 .....   | 154 |
| 4.6.35.1 | Formatos para el recojo de evidencias.....                                | 155 |
| 5        | CONCLUSIONES .....  | 156 |
| 6        | RECOMENDACIONES .....   | 157 |
| 7        | BIBLIOGRAFÍA.....   | 158 |
| 8        | ANEXOS.....   | 160 |
| 8.1      | Anexo 01: Glosario .....  | 160 |
| 8.2      | Anexo 02: Consolidado de entrevistas a 10 Establecimientos de Salud ..... | 161 |

## **INTRODUCCIÓN**

Las exigencias de un mercado cada vez más competitivo plantean nuevos desafíos, que son imposibles de alcanzar sin la incorporación de la tecnología adecuada para el manejo de la información que cada empresa desarrolla día a día, la cual está sujeta a amenazas tanto de índole externa como interna.

La información en la empresa es uno de los activos más importantes que posee y por ende se debería desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información.

En la Unidad Ejecutora 400 del sector salud de la Región Piura existen 124 Establecimientos de Salud, en los cuales la información del Aplicativo para el Registro de Formatos SIS y del Sistema de Información en Salud son unos de los pilares más importantes de cada centro de salud, teniendo que brindársele una seguridad especial a la información que mes a mes se genera.

Es por eso que la propuesta de auditoria informática a esos sistemas es de vital importancia para que cuando se presente algún tipo de inconveniente o supervisión se tenga una ayuda para saber cómo actuar frente a alguna amenaza que puede poner en riesgo la información, o en general para que se evalúe los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

# **CAPITULO 1: EL PROBLEMA DE INVESTIGACIÓN**

## **1.1 Descripción del problema**

El avance tecnológico de los sistemas y telecomunicaciones han alcanzado gran evolución, junto con eso en la misma proporción avanzan los riesgos asociados a las mismas, y hoy en día para muchas empresas del Perú, sean privadas o públicas, la seguridad de la información es un problema que poseen en común, debido a que pocas de estas empresas plantean medidas de contingencia para salvaguardar el activo más importante hoy considerado como lo es La Información.

Para el Ministerio de Salud a nivel de Unidad Ejecutora 400 de la Región Piura, como ente público del Estado Peruano, la información de todos los sistemas que maneja son de vital importancia, pero en especial la información del Aplicativo para el Registro de Formatos SIS y del Sistema de Información en Salud que se maneja por Unidad Ejecutora 400, debido a que anualmente el Ministerio de Economía y Finanzas busca medir el nivel de cumplimiento de las metas programadas cada año con la finalidad de reembolsar el dinero correspondiente para que los diversos Establecimientos de Salud puedan atender a la población de manera eficiente y eficaz, brindando todos los tipos de atenciones para intervenir a la población con atención preventiva y recuperativa, y de esa forma mejorar la salud de la población.

Es por eso que ambos sistemas son preponderantes para medir el nivel de cumplimiento de atenciones por cada Establecimiento de Salud en la región, además sirve para la toma de decisiones a nivel de gobierno central. Para todos los Establecimientos de Salud de la Unidad Ejecutora 400 de la Región Piura, la información de ambos sistemas es imprescindible, siendo motivo suficiente para preocuparse por ella y tratar de mejorar la seguridad de la información, ya que uno de los grandes problemas que se presenta en los Establecimientos de Salud es que la información está expuesta a varios riesgos, y uno de ellos es que ambos son

sistemas de escritorio, y las bases de datos se guardan en el disco duro de las computadoras, por lo cual no hay algo seguro de que la información se quede allí y no se borre, es evidente que la seguridad es un tema importante para auditar y dar posibles soluciones ante algún desastre de cualquier naturaleza.

Otro de los problemas es que los Establecimientos de Salud no poseen políticas de seguridad documentadas como por ejemplo un plan de contingencia, si algo pasa en estos momentos con la información o con el hardware, éstos correrían peligro. Es por eso que ejecutando un plan de auditoria informática se podría tener un buen manejo de riesgos previniendo cualquier tipo de inconveniente, comprendiendo requisitos de seguridad, vulnerabilidad y amenazas.

En una organización está claro que se puede mejorar solo lo que se puede medir, y frente a toda esta problemática, la Propuesta de un Plan de auditoria informática evaluaría la eficacia y eficiencia del uso correcto de los recursos informáticos para los dos sistemas en estudio, además de la gestión informática, y si se está brindando el soporte adecuado a los objetivos y metas de los sistemas para analizar el impacto que aportaría grandes beneficios a los diferentes Establecimientos de Salud, además ésta propuesta de auditoria con su implementación posterior pretende establecer lineamientos que en el futuro se puedan mejorar los ya existentes y estandarizar procesos y procedimientos ,todo ello con el fin de mejorar los sistemas que se tienen en el área de Estadística e Informática delos Establecimientos de Salud e incrementar la efectividad y productividad de dicha área. Así mismo, la propuesta de un plan de auditoria informática puede lograr que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, estructurada, eficiente y adaptada a los cambios que se producen en los riesgos, el entorno y la tecnología.



## **1.2 Formulación del problema**

¿Es posible desarrollar una Propuesta de un plan de auditoría informática para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS en los establecimientos de salud de la Unidad Ejecutora 400 en la Región Piura?

## **1.3 Objetivos de la investigación**

### **1.3.1 Objetivo General**

- Proponer un plan de auditoria informática en los establecimientos de salud de la Unidad Ejecutora 400 en la Región Piura para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS en el año 2015.

### **1.3.2 Objetivos específicos**

- Analizar los riesgos que afectan la seguridad de la información que corresponden al Sistema de Información en Salud y al Aplicativo para el Registro de Formatos SIS.
- Establecer los objetivos del plan de auditoria a proponer.
- Establecer los objetivos de control y los procedimientos de auditoría a aplicar sobre el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.
- Determinar el programa de auditoría que se utilizará de guía para ejecutar el Plan de Auditoría.

## **1.4 Justificación, importancia y beneficios de la investigación**

### **1.4.1 Justificación**

La propuesta de un plan de auditoria informática para el Sistema de Información en Salud y el Aplicativo de Registro de Formatos SIS se justifica porque permitirá la estandarización de los procesos y procedimientos con el fin de mejorar la eficiencia, eficacia y economía de cada sistema, teniendo en cuenta que la información que se maneja es la base para cada Establecimiento de Salud que está dentro de la Unidad Ejecutora 400, debido a que son evaluados económicamente por la cantidad de atenciones ingresadas en cada sistema.

### **1.4.2 Importancia**

Esta propuesta de un plan de auditoria informática para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS pretende mejorar la reducción de la cantidad de amenazas que puedan afectar a los distintos procesos de los sistemas en estudio, es decir permite conocer los riesgos asociados a las tecnologías de la información para que mediante la aplicación de normas, estándares y mejores prácticas los riesgos sean conocidos, gestionados y controlados, y de esa forma salvaguardar y manejar adecuadamente la información que día a día se ingresa aplicando una guía debidamente estructurada como lo es la propuesta del plan de auditoria informática.

### **1.4.3 Beneficiarios de la Investigación**

- Control Interno de la Dirección Regional de Salud Piura, debido a que tendrán un modelo de auditoría informática a seguir para una posterior ejecución de este plan en cada Establecimiento de Salud de la Unidad Ejecutora 400.
- La administración de cada Establecimiento de Salud en la Unidad Ejecutora 400 porque le ayudará a tener un mejor control de la gestión en

cada sistema, y así poder evitarse gastos innecesarios en mantenimiento de los mismos.

- Los digitadores de cada Establecimiento de Salud, debido a que con esta propuesta de auditoria informática se podrá llevar un mejor control de los riesgos al momento de utilizar cada sistema, y así evitar la pérdida de tiempo para digitar.

## **1.5 Hipótesis**

### **1.5.1 Hipótesis principal**

Es factible desarrollar la Propuesta de un plan de auditoria informática para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS en los establecimientos de salud de los Unidad Ejecutora 400 en la Región Piura.

#### **1.5.1.1 Identificación y operacionalización de las variables**

##### **Variable independiente**

Propuesta de un plan de auditoria informática

##### **Variable dependiente**

Desarrollar la propuesta de un plan de auditoria informática.

| VARIABLE   | DEFINICION<br>CONCEPTUAL   | INDICADOR  |
|--|--|--|
| Variable independiente: Propuesta de un plan de auditoria informática              |  |  |
| Propuesta de un plan de auditoria informática.                                     | Es el planteamiento de una guía para mantener la seguridad de los datos utilizando eficientemente los recursos y así poder evitar pérdidas que afectan al buen funcionamiento de los sistemas. | Nº de objetivos de control.  |
|  |  | Nº de actividades en los procedimientos de auditoria.  |
|  |  | Nº de técnicas utilizadas en los procedimientos de auditoria.  |
| Variable dependiente: Desarrollar la propuesta de un plan de auditoria informática |  |  |
| Desarrollar la propuesta de un plan de auditoria informática                       | Es la entrega de la propuesta del plan de auditoria informática para los sistemas en estudio.  | Nº de pautas tomas de la Norma Técnica Peruana ISO 27001:2008 y de la Guía de Control Interno del Estado Peruano |

**Tabla Nº 01: Operacionalización de las variables**

**Fuente: Elaboración propia**

## **CAPITULO 2: MARCO TEÓRICO**

### **2.1 Antecedentes**

- HUAMAN, F. (2014); En su tesis denominada **“Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implementación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano”**, logró brindar procedimientos concretos o guías para poder realizar procesos de auditoría que tengan como objetivo corroborar la implantación de la NTP 27001 en las empresas del estado peruano. Todo esto basado en la Norma Técnica Peruana NTP-ISO / IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información.
- CARBAJAL, J. (2013); En su tesis denominada **“Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano ”**, propone una metodología que permite guiar a los auditores gubernamentales del sistema nacional del control peruano en las auditorías de sistemas informáticos que se realizan en el sector público peruano, en la que aplicó la ley N° 27785 que es la ley orgánica del Sistema Nacional de Control y de la Contraloría General de la República, así como las normas de control interno
- ALIAGA, L. (2013); En su tesis denominada **“Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo”** identifica, analiza y evalúa los riesgos a los que están expuestos los activos de la entidad en estudio basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005 adoptando como framework de negocios la actual versión de COBIT, obteniendo como resultado la documentación exigida por la norma internacional para el diseño del Sistema de Gestión de Seguridad de Información.

## **2.2 Actividad empresarial**

### **2.2.1 Dirección Regional de Salud – Piura**

#### **2.2.1.1 Reseña Histórica**

La base legal del Ministerio de Salud tiene su nacimiento con la creación de la Dirección de Salubridad Pública como dependencia del Ministerio de Fomento en el 1903. Entre el año 1935 por las leyes 8124 y 9779, se crea el Ministerio de Salud Pública, Trabajo y Previsión Social basado en la estructura de la anterior Organización para posteriormente cambiar el nombre de su Institución por el nombre de Ministerio de Salud Pública. Entre el año 1945 y 1958 se reestructura el Ministerio de Salud Pública y se entrega a nivel local los servicios de Salud bajo el comando de las Unidades Sanitarias Departamentales.

#### **2.2.1.2 Misión**

La Dirección Regional de Salud Piura tiene la Misión de proteger la dignidad personal, promoviendo la salud para construir una cultura de salud y de solidaridad, previniendo las enfermedades y garantizando la atención integral de salud de todos los habitantes; cumpliendo las políticas y objetivos nacionales de salud en concertación con todos los sectores públicos y privados y otros actores sociales.

#### **2.2.1.3 Visión**

- Primacía de la persona humana sobre las instituciones.
- Nuevas dimensiones de la ciudadanía: equidad de salud y derecho a la salud.
- Reformulación de la relación Estado-Sociedad Civil.
- Descentralización y participación social.
- Revolución en las ciencias de la administración y el paso a la gerencia de calidad total y la planificación estratégica.

- Revalorización de los recursos humanos, la cultura institucional y la innovación científico-tecnológica permanente.
- Garantizar el acceso universal a los servicios de salud pública y atención individual, priorizando los sectores más pobres y vulnerables.

#### **2.2.1.4 Funciones**

- Aseguramiento financiero de la salud pública y salud integral de todas las personas
- Conducción y planeamiento estratégico sectorial de salud
- Creación de una cultura de salud sustentada en la familia como unidad básica de salud y la adquisición de capacidades y desarrollo de actitudes en las personas, para su desarrollo físico, mental y social y para la construcción de entornos saludables por la persona, la familia y la comunidad
- Creación del entorno saludable para el desarrollo de toda la población
- Desarrollo de capacidades suficientes para proteger, recuperar y mantener la salud de las personas y poblaciones, que sean afectadas por situaciones de emergencia, urgencias, desastres y/o epidemias.
- Desarrollo de las capacidades en las entidades y recursos humanos para incrementar la investigación, prestación de servicios y producción de bienes para la salud
- Desarrollo e integración de procesos y sistemas de información sectoriales, para la integración de los flujos de información de los procesos y sistemas organizacionales y la provisión de información oportuna y confiable, para la toma de decisiones por las autoridades y usuarios del Sector Salud

#### **2.2.1.5 Ámbito de ejecución**

En toda la región Piura existen 7 Unidades Ejecutoras, las cuales se detallan a continuación:





## **2.2.2 Seguro Integral de Salud**

El Seguro Integral de Salud (SIS), como Organismo Público Ejecutor (OPE), del Ministerio de Salud, tiene como finalidad proteger la salud de los peruanos que no cuentan con un seguro de salud, priorizando en aquellas poblacionales vulnerables que se encuentran en situación de pobreza y pobreza extrema.

De esta forma, estamos orientados a resolver la problemática del limitado acceso a los servicios de salud de nuestra población objetivo, tanto por la existencia de barreras económicas, como las diferencias culturales y geográficas. Pero el SIS también busca mejorar la eficiencia en la asignación de los recursos públicos e implementando instrumentos de identificación del usuario, priorizando el componente materno infantil.

### **2.2.2.1 Misión**

Somos una Institución Administradora de Fondos de Aseguramiento en Salud - IAFAS pública que administra fondos y gestiona riesgos de salud, a través de una gestión eficiente, financiando siniestros, fomentando la cultura de aseguramiento y de prevención en salud para la satisfacción de la población objetivo.

### **2.2.2.2 Visión**

Ser reconocida como una institución líder en aseguramiento público en salud al servicio de las personas.

### **2.2.2.3 Valores Institucionales**

- **Responsabilidad**

El SIS y sus trabajadores son conscientes que sus decisiones pueden generar valor agregado en sus vidas y en los que nos rodean y que la responsabilidad es un acto o una decisión que realizamos en forma convincente y con un propósito de servicio en salud de la población.

- **Equidad**

El SIS y sus trabajadores se preocupan por brindar protección financiera a sus afiliados de acuerdo a sus necesidades de salud.

- **Compromiso**

Los trabajadores del SIS muestran una actitud que busca superar las dificultades para alcanzar los objetivos con plena identificación institucional.

- **Vocación de Servicio**

El SIS y sus trabajadores se preocupan de atender con un trato oportuno, humano y de calidad a los ciudadanos que requieren de afiliación y financiamiento.

- **Ética**

Los trabajadores del SIS demuestran un comportamiento honesto, probo, transparente y de conducta intachable en su desempeño.

### **2.2.2.4 Objetivos**

Los Objetivos funcionales del SIS en el ámbito sectorial, son los siguientes:

- a) Construir un sistema de aseguramiento público sostenible que financie servicios de calidad para la mejora del estado de salud de las personas a través de la disminución de la tasa de morbimortalidad.

- b) Promover el acceso con equidad de la población no asegurada a prestaciones de salud de calidad, dándole prioridad a los grupos vulnerables y en situación de pobreza y extrema pobreza.
- c) Implementar políticas que generen una cultura de aseguramiento en la población.

(Recuperado de <http://www.sis.gob.pe/>)

### **2.2.3 Base legal de la Unidad Ejecutora 400**

- Ley N° 27657 Ley del Ministerio de Salud
- Ley N° 27783 Ley de Bases de la Descentralización
- Ley N° 27444 Ley del Procedimiento Administrativo General
- Ley N° 28273 Ley del Sistema de Acreditación de los Gobiernos Regionales y Locales
- Ley N° 27813 Ley del Sistema Nacional Coordinado y Descentralizado en Salud
- Ley N° 27867 Ley Orgánica de Gobierno Regionales
- Ley N° 28411 Ley General del Sistema Nacional de Presupuesto
- Ley N° 29951 Ley de Presupuesto del Sector Público para el año fiscal 2013
- **Ley N° 27785 Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República**
- Decreto Supremo N° 023-2005-SA, aprueba el Reglamento de Organización y Funciones del Ministerio de Salud y su modificatoria, Decreto Supremo N° 007-2006-SA.

Se tendrá en cuenta la Ley N° 27785, debido a que en base a esta ley se trabaja la auditoría de control interno. Sin embargo, no se ha realizado ninguna auditoría oficial al Sistema de Información en Salud en la Unidad Ejecutora 400 de la Región Piura en años anteriores.

(Recuperado de

[http://www.diresapiura.gob.pe/drsp/institucional/docgestion/ROF\\_2013\\_Direccion%20Regional%20de%20Salud%20Piura.pdf](http://www.diresapiura.gob.pe/drsp/institucional/docgestion/ROF_2013_Direccion%20Regional%20de%20Salud%20Piura.pdf))

## **2.2.4 Resolución Jefatural N° 170 – 2012 / Sis**

### **2.2.4.1 Alcance**

Es la directiva que establece el proceso de control presencial posterior de las prestaciones de salud financiadas por el Seguro Integral de Salud.

### **2.2.4.2 Finalidad**

Establecer normas y procedimientos orientados a contribuir al control de las prestaciones de salud y propiciar el mejoramiento continuo de la calidad de información correspondiente a la atención brindada a los asegurados del SIS.

### **2.2.4.3 Objeto**

Establecer las disposiciones necesarias para la aplicación de la auditoria presencial posterior de la información de prestaciones de Salud financiadas por el Seguro Integral de Salud.

### **2.2.4.4 PCPP: Proceso de Control Presencial Posterior de las prestaciones de Salud**

Consiste en la evaluación y verificación documentaria in situ de las prestaciones de salud financiadas por el SIS y registradas en el Aplicativo de Registro de Formatos SIS por los establecimientos de salud. Este tipo de proceso consta de dos fases:

- Evaluación de la conformidad del registro de formato único de atención.
- Evaluación de la conformidad de la prestación de salud.

#### 2.2.4.5 Auditoria ejecutada

Se realizó una auditoria informática por trimestre en el año 2014, en la que se auditó la información ingresada en el Aplicativo de Registro de Formatos SIS, teniendo como meta no llegar a sobrepasar el 50% de fichas rechazadas, y se obtuvo como resultado de rechazo el 69% de fichas ingresadas en el aplicativo a nivel de Unidad Ejecutora. A continuación se detalla en el siguiente cuadro:

| INDICADOR  | FORMULA  | VALOR<br>ALCANZADO | PORCENTAJE<br>ALCANZADO | META |
|--|--|--------------------|-------------------------|------|
| Porcentaje de<br>formatos SIS<br>rechazados<br>por la<br>auditoria<br>informática. | Nº acumulado de<br>prestaciones<br>rechazadas por la<br>auditoria en el<br>año 2014 X100 | 4707               | 69%                     | 50%  |
|  | Nº acumulado de<br>prestaciones<br>evaluadas por la<br>auditoria<br>informática.         | 6725               |                         |      |

**Tabla Nº 2: Evaluación de auditoria en la Unidad Ejecutora 400.**

**Fuente: Resolución Jefatural Nº 170**

**(Resolución Jefatural Nº 170, 2012 pp 4-7)**

### 2.3 Bases teóricas

#### 2.3.1 Auditoria en sistemas de información

##### 2.3.1.1 Auditoria

**Una de las definiciones de auditoría es:**

Auditoría es un proceso para determinar el cumplimiento con los requerimientos, planes y contrato, según aplique. Se indica además que este proceso puede ser empleado por

cualesquiera de las dos partes, donde una de ellas (la auditora) audita los productos software o actividades de la otra parte (la auditada). Según ISACA (2008), la auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

(NTP-ISO/IEC 12207, 2006 p. 72)

#### **2.3.1.2 Tipos de Auditorías**

**Una de las clasificaciones que se propone es:**

##### **Auditorías por su lugar de aplicación**

- Auditoría externa
- Auditoría interna

##### **Auditorías por su área de aplicación**

- Auditoría financiera
- Auditoría administrativa
- Auditoría operacional
- Auditoría integral
- Auditoría gubernamental
- Auditoría de sistemas

##### **Auditorías especializadas en áreas específicas**

- Auditoría al área médica (evaluación médico-sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoría laboral
- Auditoría de proyectos de inversión
- Auditoría a la caja chica o caja mayor (arqueos)

- Auditoría al manejo de mercancías (inventarios)
- Auditoría ambiental
- Auditoría de sistemas

#### **Auditoría de sistemas computacionales**

- Auditoría informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría alrededor de la computadora
- Auditoría de la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsourcing
- Auditoría ergonómica de sistemas computacionales

**(MUÑOZ, C.; 2002 pp. 12-13)**

#### **2.3.1.3 Auditoría Informática**

**Uno de los conceptos encontrados es:**

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución,

incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

(MUÑOZ, C.; 2002 p. 19)

## **2.3.2 Sistemas de control**

### **2.3.2.1 Control interno**

El control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente. Su ejercicio es previo, simultáneo y posterior. El control interno previo y simultáneo compete exclusivamente a las autoridades, funcionarios y servidores públicos de las entidades como responsabilidad propia de las funciones que le son inherentes, sobre la base de las normas que rigen las actividades de la organización y los procedimientos establecidos en sus planes, reglamentos, manuales y disposiciones institucionales, los que contienen las políticas y métodos de autorización, registro, verificación, evaluación, seguridad y protección. El control interno posterior es ejercido por los responsables superiores del servidor o funcionario ejecutor, en función del cumplimiento de las disposiciones establecidas, así como por el órgano de control institucional según sus planes y programas anuales, evaluando y verificando los aspectos administrativos del uso de los recursos y bienes del Estado, así como la gestión y ejecución llevadas a cabo, en relación con las metas trazadas y resultados obtenidos.

### **2.3.2.2 Control externo**

Se entiende por control externo el conjunto de políticas, normas, métodos y procedimientos técnicos, que compete aplicar a la Contraloría General u otro órgano del Sistema por encargo



designación de ésta, con el objeto de supervisar, vigilar y verificar la gestión, la captación y el uso de los recursos y bienes del Estado. Se realiza fundamentalmente mediante acciones de control con carácter selectivo y posterior.

(Recuperado de [http://www.app.minsa.gob.pe/denuncias\\_oci/LEY%2027785.pdf](http://www.app.minsa.gob.pe/denuncias_oci/LEY%2027785.pdf))

### **2.3.3 Evaluación de riesgos**

La Evaluación de Riesgos en una Empresa considera todos aquellos riesgos relevantes que pueden afectar su funcionamiento y operación. El auditor estará más interesado en la Evaluación de Riesgos de una Entidad relacionados con la Información Financiera. Los Riesgos Relevantes a la información financiera, incluyen eventos o circunstancias externas o internas que pueden ocurrir y afectar la habilidad de la entidad en el Registro, Procesamiento, Agrupación o Reporte de Información.

Algunos de los riesgos relevantes que pueden presentarse en una Empresa, y sobre los cuales el auditor debe poner especial interés por el efecto que pueden tener en la información financiera son:

- Cambios en el ambiente operativo
- Nuevo personal
- Sistemas de información nuevos o rediseñados
- Crecimientos acelerados
- Nuevas tecnologías
- Nuevas líneas, productos o actividades
- Reestructuraciones Corporativas
- Cambio en pronunciamientos contables
- Personal con mucha antigüedad
- Operaciones en el extranjero

La Evaluación de Riesgos que realiza la entidad difiere de la consideración de riesgos de auditoría que realiza el auditor en una

auditoria de estados financieros cuyo enfoque es identificar aquellas situaciones o riesgos que pueden estar afectando los estados financieros de la Empresa.

(Recuperado

de

<http://www.ccpm.org.mx/avisos/boletines/boletinauditoria3.pdf>)

#### 2.3.4 Seguridad de la Información

**Una de las conceptualizaciones sobre seguridad de la información es:**

La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información (SI) como: La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización. Además, también pueden estar involucradas otras propiedades como son: la autenticidad, la responsabilidad, el no-repudio y la confiabilidad.

Es decir, estos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación:

**Confidencialidad.** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

**Integridad.** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Para garantizar la integridad de la información el remitente debe estar siempre autenticado. Esta se puede ver afectada por problemas de hardware, software, virus o personas malintencionadas.

**Disponibilidad.** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

(LOPEZ, A;2011p. 15)

## **2.3.5 Amenazas y vulnerabilidades**

### **2.3.5.1 Amenazas**

**Una de las definiciones es:**

De acuerdo con la normas ISO 27000, se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización. Alexander y otros (2007), coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etcétera.
- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.
- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware o de red.

**(LOPEZ, A; 2011 pp. 16 - 17)**

### **2.3.5.2 Vulnerabilidades**

**Uno de los conceptos es:**

Las vulnerabilidades están asociadas a debilidades de los activos de información. La vulnerabilidad en el contexto de los sistemas de información es considerada como la ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición.

Las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información. Esto es lo que para expertos en temas de seguridad de información se conoce como la relación causa-efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será el de integrar estos elementos para analizar y definir los niveles de riesgo que luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

**(LOPEZ, A; 2011p.17)**

### **2.3.6 Sistemas de información**

**Una interpretación sobre sistemas de información es:**

Un Sistema de Información (SI) es un conjunto de componentes interrelacionados para recolectar, manipular y diseminar datos e información y para disponer de un mecanismo de retroalimentación útil en el cumplimiento de un objetivo. Todos interactuamos en forma cotidiana con sistemas de información, para fines tanto personales como profesionales; utilizamos cajeros automáticos, los empleados de las tiendas registran nuestras compras sirviéndose de códigos de barras y escáner u obtenemos información en módulos equipados con pantallas sensibles al tacto, las muy famosas touchscreen. Las principales compañías gastan en la actualidad más de 1 000 millones de dólares al año en tecnología de información y el futuro dependeremos aún más de los sistemas de información.

Hay tres actividades en un sistema de información que producen la información que las organizaciones necesitan para tomar decisiones, controlar operaciones, analizar problemas y crear nuevos productos o servicios. Estas actividades son entrada, procesamiento y salida. La entrada captura o recolecta datos en bruto tanto al interior de la organización como de su entorno externo. El procesamiento convierte esta entrada de datos en una forma significativa. La salida transfiere la información procesada a la gente que lo usará o a las actividades para las que se utilizará. Los sistemas de información también requieren retroalimentación que es la salida que se devuelve al personal adecuado de la organización para ayudarle a evaluar o corregir la etapa de entrada.

**(CERENI, My PRA, P; 2012p. 15)**

## **2.3.7 Plan de auditoría informática**

### **2.3.7.1 Objetivo de Control**

#### **Concepto**

Un "Objetivo de Control", es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática y sistemas de información.

Estos objetivos de control de tecnología informática han sido organizados por proceso / actividad, pero también se facilita la entrada a partir de cualquier punto de vista estratégico, además para lograr enfoques combinados o globales, tales como instalación / implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de

tecnología informática por un proceso. Para mayor facilidad los Objetivos de Control, dentro del COBIT han sido definidos en una manera genérica, sin depender de la plataforma técnica.

**(Recuperado de <http://especialistas.org.ar/cie/files/material/cobit.pdf> - Definición de Objetivos de Control)**

### **2.3.7.2 Procedimiento de Auditoría**

#### **Concepto**

Al conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.

La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría. El auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.

En General los procedimientos de auditoría permiten:

- Obtener conocimientos del control interno.
- Analizar las características del control interno.
- Verificar los resultados de control interno.
- Fundamentar conclusiones de la auditoría.

Por esta razón el auditor deberá aplicar su experiencia y decidir cuál técnica o procedimiento de auditoría serán los más indicados para obtener su opinión

(En: <http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s03.html>-  
Definición de procedimiento)

## **2.4 Normatividad**

### **2.4.1 LEY N° 27785: Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la Republica.**

#### **2.4.1.1 Ámbito de aplicación**

Las normas contenidas en la presente Ley y aquellas que emita la Contraloría General son aplicables a todas las entidades sujetas a control por el Sistema, independientemente del régimen legal o fuente de financiamiento bajo el cual operen. Dichas entidades sujetas a control por el Sistema, que en adelante se designan con el nombre genérico de entidades, son las siguientes:

- El Gobierno Central, sus entidades y órganos que, bajo cualquier denominación, formen parte del Poder Ejecutivo, incluyendo las Fuerzas Armadas y la Policía Nacional, y sus respectivas instituciones.
- Los Gobiernos Regionales y Locales e instituciones y empresas pertenecientes a los mismos, por los recursos y bienes materia de su participación accionaria.
- Las unidades administrativas del Poder Legislativo, del Poder Judicial y del Ministerio Público.
- Los Organismos Autónomos creados por la Constitución Política del Estado y por ley, e instituciones y personas de derecho público.
- Los organismos reguladores de los servicios públicos y las entidades a cargo de supervisar el cumplimiento de los compromisos de inversión provenientes de contratos de privatización.
- Las empresas del Estado, así como aquellas empresas en las que éste participe en el accionariado, cualquiera sea la forma societaria

que adopten, por los recursos y bienes materia de dicha participación.

- Las entidades privadas, las entidades no gubernamentales y las entidades internacionales, exclusiva mente por los recursos y bienes del Estado que perciban o administren. En estos casos, la entidad sujeta a control, deberá prever los mecanismos necesarios que permitan el control detallado por parte del Sistema.

#### **2.4.1.2 Acción de control**

La acción de control es la herramienta esencial del Sistema, por la cual el personal técnico de sus órganos conformantes, mediante la aplicación de las normas, procedimientos y principios que regulan el control gubernamental, efectúa la verificación y evaluación, objetiva y sistemática, de los actos y resultados producidos por la entidad en la gestión y ejecución de los recursos, bienes y operaciones institucionales.

(Recuperado de  
[http://www.app.minsa.gob.pe/denuncias\\_oci/LEY%2027785.pdf](http://www.app.minsa.gob.pe/denuncias_oci/LEY%2027785.pdf))

### **2.4.2 MAGU: Manual De Auditoria Gubernamental**

#### **2.4.2.1 Concepto**

El Manual de Auditoría Gubernamental, en adelante MAGU, es el documento normativo fundamental que define las políticas y las orientaciones para el ejercicio de la auditoría gubernamental en el Perú. Es aprobado por el Contralor General de la República en su calidad de titular del órgano rector del Sistema Nacional de Control.

#### **2.4.2.2 Objetivos**

- Establecer los postulados, criterios, metodología y los procesos que requiere la auditoría gubernamental, con el propósito de uniformar el trabajo de los auditores y promover



un mayor grado de eficiencia, efectividad y economía en el desarrollo de la auditoría gubernamental en su conjunto.

- Determinar los criterios básicos que permitan en el futuro llevar a cabo el control de calidad de la auditoría gubernamental que realicen los auditores del Sistema Nacional de Control (Contraloría General de la República, Órganos de Auditoría Interna del sector público y las Sociedades de Auditoría Independiente, previamente designadas por el Organismo Superior de Control).
- Aplicar las normas de auditoría gubernamental-NAGU aprobadas por la Contraloría General de la República y aquella normatividad que sea pertinente, estableciendo criterios modernos para el desarrollo de la auditoría gubernamental.
- Proporcionar un importante texto de consulta para los profesionales que ejercen la auditoría gubernamental, y promover la formación de auditores en las Universidades del país.
- Permitir el dictado de programas de entrenamiento profesional en la Escuela Nacional de Control, para los profesionales que ejercen la auditoría gubernamental aplicando el marco conceptual y terminología uniforme.

#### **2.4.2.3 Alcance**

- Comprende la auditoría financiera, la auditoría de gestión y examen especial, de acuerdo con el marco conceptual de las normas de auditoría gubernamental aprobado por la Contraloría General de la República.
- El MAGU es aplicable a los auditores de la Contraloría General de la república, a los auditores internos de las entidades del Sector Público Nacional y a los auditores de las sociedades de auditoría independiente, cuando sean designados para examinar a entidades del Estado.

- Corresponde a la Contraloría General de la República ejercer el control de calidad de la auditoría gubernamental y determinar si el trabajo de los auditores fue concluido, de acuerdo con la normatividad, criterios y metodología establecida en el Manual de Auditoría Gubernamental-MAGU.

**(MAGU, (1998) pp.3 -4)**

## **2.4.3 NAGU**

### **2.4.3.1 Concepto**

Las Normas de Auditoría Gubernamental - NAGU son los criterios que determinan los requisitos de orden personal y profesional del auditor, orientados a uniformar el trabajo de la Auditoría gubernamental y obtener resultados de calidad. Constituyen un medio técnico para fortalecer y uniformar el ejercicio profesional del auditor gubernamental y permiten la evaluación del desarrollo y resultados de su trabajo, promoviendo el grado de economía eficiencia y eficacia en la gestión de la entidad auditada. Se fundamentan en la Ley del Sistema Nacional de Control, su Reglamento y en las Normas de Auditoría Generalmente Aceptadas. Las NAGA son aplicables en su totalidad cuando se trata de una Auditoría financiera, y en lo aplicable, en una Auditoría de asuntos financieros en particular y otros exámenes especiales. La Auditoría de gestión requiere, sin embargo normas complementarias y específicas para satisfacer las necesidades propias de los citados exámenes.

Los auditores deben seleccionar y aplicar las pruebas y demás procedimientos de auditoría que, según su criterio profesional, sean apropiadas en las circunstancias para cumplir los objetivos de cada auditoría. Esas pruebas y procedimientos deben planearse de tal modo que permitan obtener evidencia suficiente,

competente y relevante para fundamentar razonablemente las opiniones y conclusiones que se formulen en relación con los objetivos de la Auditoría.

#### **2.4.3.2 Programas de auditoría**

Para cada auditoría deben prepararse programas específicos que incluyan objetivos, alcance de la muestra, procedimientos detallados y oportunidad de su aplicación, así como el personal encargado de su desarrollo. Los programas de auditoría comprenden una relación ordenada de procedimientos a ser aplicados en el proceso de la auditoría, que permitan obtener las evidencias competentes y suficientes para alcanzar el logro de los objetivos establecidos. Se desarrollan a partir del conocimiento de la entidad y sus sistemas. El auditor se apoya en este conocimiento para establecer la naturaleza, oportunidad y alcance de los procedimientos a aplicar. Su flexibilidad debe permitir modificaciones, mejoras y ajustes que a juicio del auditor encargado y supervisor se consideren pertinentes durante el curso de la auditoría. Los programas de auditoría guían la acción del auditor y sirven como elemento para el control de la labor realizada. Deben también permitir la evaluación del avance del examen y la correcta aplicación de los procedimientos, cautelando que la consecución de los resultados este de acuerdo con los objetivos propuestos. El programa de auditoría debe ser lo suficientemente detallado de manera que sirva de guía y como medio para controlar la adecuada ejecución del trabajo. La responsabilidad de la elaboración de los respectivos programas corresponde al auditor encargado y supervisor

### **2.4.3.3 Archivo permanente**

Para cada entidad sujeta a control se debe implantar, organizar y mantener actualizado el archivo permanente. El Archivo Permanente está conformado por un conjunto orgánico de documentos que contienen copias y/o extractos de información de interés, de utilización continua o necesaria para futuros exámenes, básicamente relacionada con:

- Ley orgánica de la entidad y normas legales que regulan su funcionamiento
- Organigrama aprobado
- Reglamento de Organización y Funciones - ROF aprobado
- Manual de Organización y Funciones - MOF aprobado
- Manual de Procedimientos aprobado
- Flujo gramas de las principales actividades de la entidad
- Plan Operativo Institucional
- Presupuesto institucional, incluyendo modificaciones y evaluaciones
- Estados financieros
- Informes de auditoría
- Denuncias
- Plan Anual de Control, incluyendo reprogramaciones
- Informe de evaluación del Plan Anual
- Resumen de las decisiones más importantes adoptadas por la Alta Dirección
- Resoluciones y Directivas emitidas por la entidad
- Convenios y Contratos trascendentes.

### **2.4.3.4 Estudio y evaluación de control interno**

El sistema de control interno comprende el plan de organización, los métodos, procedimientos y la función de auditoría interna establecidos dentro de una entidad pública, para salvaguardar su patrimonio contra el mal gasto, pérdida y uso indebido, verificar la exactitud y veracidad dela información

financiera y administrativa promover la eficiencia en las operaciones y comprobar el cumplimiento de los objetivos y políticas institucionales así como de la normativa aplicable. Un apropiado sistema de control interno, también permite detectar posibles deficiencias y aquellos aspectos relacionados con la existencia de delitos, de ser el caso.

La administración de la entidad es responsable de implantar y mantener un sistema eficaz de control interno, cuya estructura comprende:

- a) Ambiente de control, que se refiere a la disposición general, actitud vigilante y acciones adoptadas por parte de la administración con respecto al control y su importancia para la entidad.
- b) Sistemas de Información y registro, consiste en los métodos y registros establecidos para identificar reunir, analizar, clasificar, registrar e informar las transacciones de una entidad.
- c) Procedimientos de control, consisten en las políticas y procedimientos adicionales establecidos por la administración para lograr una razonable seguridad de e los objetivos específicos de la entidad serán alcanzados.

El estudio y evaluación del sistema de control interno tiene por objeto conocer con mayor precisión aquellos aspectos de importancia de la organización y funcionamiento de la entidad, así como, efectuar los ajustes de los programas y la aplicación detallada de procedimientos de auditoría, especialmente en las aéreas críticas, que servirán como base para el establecimiento de los objetivos y alcance de la auditoría, la formulación de recomendaciones a considerarse en el informe y la determinación del grado de confianza de los controles implantados por la entidad. El estudio y evaluación del sistema de control interno debe ser llevado a cabo de acuerdo al tipo de

auditoría que se ejecute, sea financiera, de gestión o se trate de exámenes especiales.

Los auditores podrán evaluar, hasta donde sea necesario para cumplir los objetivos de la auditoría aquellas políticas, procedimientos, prácticas y controles que sean aplicables a los programas, funciones y actividades que sean materia de la auditoría. El relevamiento de información del sistema de control interno debe documentarse adecuadamente, teniendo en cuenta la forma en que se presente la información y, el criterio del auditor.

La evaluación del sistema de control interno comprende dos etapas:

1. Obtención de información acerca de su funcionamiento.
2. Comprobación de que los controles identificados funcionan efectivamente y logran sus objetivos.

En caso de encontrarse computarizados los sistemas de información y registro, el auditor debe establecer si los controles internos están funcionando apropiadamente, a fin de brindarle confianza respecto a la integridad de los datos procesados mediante medios informáticos. Al término de esta evaluación el auditor emitirá el documento denominado Memorandum de Control Interno, el cual estará dirigido al titular de la entidad.

**(Recuperado de <http://www.perucontadores.com/audgub/NAGU.pdf>)**

## 2.4.4 NTP ISO/IEC 27001:2008

### 2.4.4.1 Concepto

Esta Norma Técnica Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar en efectivo Sistema de Gestión de Seguridad de la Información ISMS, por sus siglas en Inglés (Information Security Management System). La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que estos y sus sistemas de soporte cambien a lo largo del tiempo, así como que las situaciones simples requieren soluciones ISMS simples.

Esta Norma Técnica Peruana puede usarse en el ámbito interno y externo de las organizaciones.

- **Enfoque de Proceso:** Esta Norma Técnica Peruana promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, mantener y mejorar la efectividad de un ISMS en la organización. Una organización debe identificar y administrar varias actividades con el fin de funcionar efectivamente. Cualquier actividad que administre y use recursos para lograr la transformación de entradas en salidas, puede ser considerado un proceso. Con frecuencia la salida de un proceso se convierte en la entrada del proceso siguiente.

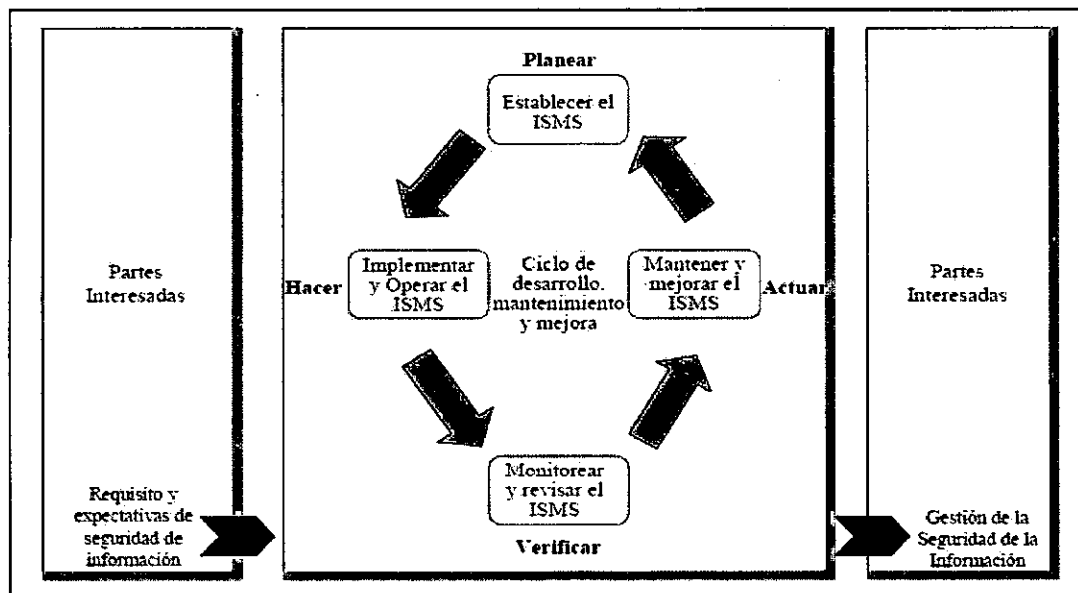
La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su administración se define como un enfoque de proceso.

El enfoque de proceso alienta a sus usuarios a enfatizar la importancia de:

- ✓ Entender los requisitos de seguridad de información de negocios y la necesidad de establecer políticas y objetivos para la seguridad de la información.
- ✓ Implementar y operar controles en el contexto de administrar el riesgo total del negocio de una organización.
- ✓ Monitorear y revisar el desempeño y efectividad del ISMS
- Y
- ✓ Mejoramiento continuo basado en la medición de objetivos.

#### 2.4.4.2 Sistema de seguridad de la información

La organización desarrollará, implementará, operará, monitoreará, revisará, mantendrá y continuará la mejora de un ISMS documentado dentro del contexto de las actividades y riesgos totales de la organización. Para los fines de esta Norma Técnica Peruana, el proceso usado se basa en el modelo PDCA mostrado a continuación:



**Figura N° 2: Modelo PDCA aplicado al proceso ISMS**  
**Fuente: NTP/ISO 27001:2008**

(NTP/ISO 27001; 2008 pp. 5-6)



## **2.4.5 Guía de control interno para el sector público**

### **2.4.5.1 Concepto**

Las Normas de Control Interno, constituyen lineamientos, criterios, métodos y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa u operativa de las entidades, incluidas las relativas a la gestión financiera, logística, de personal, de obras, de sistemas de información y de valores éticos, entre otras. Se dictan con el propósito de promover una administración adecuada de los recursos públicos en las entidades del Estado.

### **2.4.5.2 Objetivos**

La guía tiene como objetivo principal promover de lineamientos, herramientas y métodos a las entidades del Estado para la implementación de los componentes que conforman el Sistema de Control Interno (SCI) establecido en las Normas de Control Interno (NCI).

Adicionalmente, también se pueden señalar los siguientes objetivos:

- Servir de referencia para la implementación o adecuación del SCI, en el marco de las NCI.
- Promover la aplicación de una estructura de control interno uniforme que se adapte a cada entidad.
- Exponer con mayor amplitud los conceptos utilizados en las NCI.

### **2.4.5.3 Ámbito de aplicación**

La Guía para la Implementación se aplica a todas las entidades comprendidas en el ámbito de competencia del SNC, bajo la supervisión de los titulares de las entidades y de los jefes

responsables de la administración gubernamental o de los funcionarios que hagan sus veces.

La presente Guía ofrece una estructura y metodología enunciativa mas no limitativa, que sirve de marco de referencia para que las entidades desarrollen la implementación de su SCI de manera homogénea en lo general y de acuerdo con su naturaleza, cultura organizacional, complejidad operativa, atribuciones, circunstancias, presupuesto, infraestructura, entorno normativo y nivel de automatización que le corresponde a cada entidad pública en lo particular. Por lo tanto, para implementar el SCI, las entidades desarrollarán etapas de acuerdo con su funcionamiento y dentro de los plazos que establezca la CGR. Para dicho fin se empezará con la sensibilización del personal en el tema de Control Interno, para pasar luego al desarrollo de un diagnóstico que permita determinar las brechas existentes que conduzcan al establecimiento de los lineamientos, políticas y controles necesarios para la implementación del SCI. Adicionalmente, la implementación de un SCI eficaz dependerá de una constante autoevaluación y un mejoramiento continuo de las políticas de control.

Finalmente, debe destacarse que el contenido de la Guía no interfiere ni se contrapone con las disposiciones establecidas en la legislación actual ni limita la normativa dictada por las entidades competentes con respecto a los sistemas administrativos del Estado, sino que complementa al adecuado establecimiento e implementación del SCI en la organización.

#### **2.4.5.4 Clasificación del riesgo**

Durante el proceso de identificación del riesgo se recomienda hacer una clasificación de los mismos teniendo en cuenta los siguientes conceptos:

##### **Riesgo estratégico**

Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas y el diseño y conceptualización de la entidad por parte de la Alta Dirección.

##### **Riesgo operativo**

Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura organizacional, en la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

##### **Riesgo Financiero**

Se relacionan con el manejo de los recursos de la entidad e incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad.

##### **Riesgos de cumplimiento**

Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

### **Riesgos de tecnología**

Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales y futuras y soporte el cumplimiento de su misión.

#### **2.4.5.5 Valoración de los riesgos**

La valoración de los riesgos se efectuará con base en la información obtenida en el registro de riesgos, elaborado en la etapa de identificación, con el fin de obtener información para determinar el nivel de riesgo y las acciones que se van a implementar.

**Probabilidad:** La posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya materializado.

**Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo. A continuación se presentan las escalas que pueden implementarse para analizar los riesgos.

#### **Análisis cualitativo**

Constituye la utilización de escalas descriptivas para demostrar la magnitud de consecuencias potenciales y su posibilidad de ocurrencia. Las escalas a utilizar estarán en razón de la evaluación de la probabilidad e impacto de los riesgos. La evaluación de probabilidad de los riesgos investiga la probabilidad de ocurrencia de cada riesgo específico. La evaluación del impacto de los riesgos investiga el posible efecto sobre los objetivos, como tiempo, costo, alcance o calidad.

En la escala de medida cualitativa de **PROBABILIDAD** se deberán establecer las categorías a utilizar y la descripción de cada una de ellas.

| <b>Categoría</b>  | <b>Definición</b>   |
|-------------------|---|
| <b>PROBABLE</b>   | Es muy frecuente la materialización del riesgo o se presume que llegara a materializarse        |
| <b>POSIBLE</b>    | Es frecuente la materialización del riesgo o se presume que posiblemente se podrá materializar. |
| <b>IMPROBABLE</b> | Es poco frecuente la materialización del riesgo o se presume que no llegara a materializarse.   |

**Tabla N° 3: Escala de medida cualitativa de la probabilidad.**  
**Fuente: Guía de Control Interno (2008)**

#### **Análisis cuantitativo**

Representa los valores numéricos para la elaboración de tablas de registro de riesgos; la calidad del análisis depende de lo precisas y completas que estén las cifras utilizadas. La forma en la cual la probabilidad y el impacto son expresadas y las formas por las cuales ellos se combinan para proveer el nivel de riesgo puede variar de acuerdo al tipo de riesgo.

| <b>Probabilidad de ocurrencia</b> | <b>Nivel</b> |
|-----------------------------------|--------------|
| 0-25                              | Improbable   |
| 26-70                             | Posible      |
| 71-100                            | Probable     |
|                                   |              |
| <b>Impacto</b>                    | <b>Nivel</b> |
| 0-25                              | Leve         |
| 26-70                             | Moderado     |
| 71-100                            | Desastroso   |

**Tabla N° 4: Escalas cuantitativas de probabilidad e impacto**  
**Fuente: Guía de Control Interno (2008)**

#### **2.4.5.6 Matriz de probabilidad e impacto**

Los riesgos pueden ser priorizados para un análisis cuantitativo posterior y para las respuestas posteriores basándose en su calificación. Las calificaciones son asignadas a los riesgos

basándose en la probabilidad y el impacto evaluados. La evaluación de la importancia de cada riesgo y, por consiguiente, de su prioridad generalmente se realiza usando una tabla de búsqueda o una matriz de probabilidad e impacto. Dicha matriz especifica combinaciones de probabilidad e impacto que llevan a la calificación de los riesgos como aceptable, tolerable, moderado, importante e inaceptable.

|              |            |   | IMPACTO              |                        |                         |
|--------------|------------|---|----------------------|------------------------|-------------------------|
|              |            |   | 1                    | 2                      | 3                       |
|              |            |   | LEVE                 | MODERADO               | DESASTROSO              |
| PROBABILIDAD | Probable   | 3 | 3<br>Riesgo Moderado | 6<br>Riesgo importante | 9<br>Riesgo inaceptable |
|              | Posible    | 2 |                      | 4<br>Riesgo moderado   | 6<br>Riesgo importante  |
|              | Improbable | 1 |                      |                        | 3<br>Riesgo moderado    |

**Tabla N° 5: Matriz de probabilidad e impacto**

**Fuente: Guía de Control Interno (2008)**

La puntuación del riesgo ayuda a guiar las respuestas a los riesgos.

| Nivel de Riesgo    | Descripción   |
|--------------------|---|
| Riesgo Inaceptable | Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Dirección.   |
| Riesgo Importante  | Se requiere atención de la alta dirección. Planes de tratamiento requeridos, implementados y reportados a los jefes de las oficinas, divisiones, entre otros. |
| Riesgo Moderado    | Debe ser administrado con procedimientos normales de control.   |
| Riesgo Tolerable   | Menores efectos que pueden ser fácilmente remendados. Se administra con procedimientos rutinarios.  |
| Riesgo Aceptable   | Riesgo insignificante. No se requiere ninguna acción.   |

**Tabla N° 6: Descripción de niveles de riesgo**

**Fuente: Guía de Control Interno (2008)**

#### **2.4.5.7 Riesgo residual**

El riesgo residual es aquél que permanece después que la Dirección toma las acciones de control necesarias para reducir la probabilidad y consecuencia del riesgo.

El riesgo residual podrá ser valorado tomando en consideración, los riesgos inicialmente evaluados contra aquellas respuestas y acciones de control que minimizaron dicho riesgo, para esto se tendrá que determinar la eficacia de las acciones de control implementadas o existentes, permitiendo así determinar el adecuado riesgo residual.

Para efectos prácticos de la determinación del riesgo residual se considerará los siguientes criterios:

| <b>Criterios</b>                        | <b>Valoración del riesgo residual</b>        |
|---|--|
| No existen actividades de control       | Se mantiene el nivel de riesgo inicial       |
| Existen actividades de control          | Se reduce en un nivel del riesgo inicial     |
| Existen actividades de control eficaces | Se reduce en dos niveles del riesgo inicial. |

**Tabla N° 7: Criterios de valoración para riesgo residual**  
**Fuente: Guía de control Interno (2008)**

**(Guía para la implementación del sistema de control interno de las entidades del estado peruano; 2008 pp. 65-83)**

## **CAPÍTULO 3: DIAGNOSTICO SITUACIONAL DE LOS SISTEMAS DE INFORMACIÓN**

### **3.1 Descripción del Sistema de Información en Salud**

#### **3.1.1 Descripción General**

El sistema de información en Salud fue creado por la Oficina General de Estadística e Informática de la Dirección Regional de Salud Piura, actualmente se trabaja con la versión HIS\_VER\_3.05-2011. En dicho sistema se digita la información de la producción de cada profesional de la salud, en las diferentes estrategias sanitarias como lo son:

- Estrategia Sanitaria de Planificación Familiar
- Estrategia Sanitaria de Materno Perinatal
- Estrategia Sanitaria de Inmunizaciones
- Estrategia Sanitaria de Daños no transmisibles
- Estrategia Sanitaria de Prevención y control de tuberculosis
- Estrategia Sanitaria de Salud Bucal
- Estrategia Sanitaria de Salud Mental y Cultura de Paz
- Estrategia Sanitaria de Salud Ocular
- Estrategia Sanitaria de Zoonosis
- Etapa de Vida Adolescente
- Etapa de Vida Niño
- Programa de prevención y control de cáncer
- Salud Ambiental
- Salud Familiar

Objetivos del Sistema:

- Servir de instrumento que facilite el ingreso, consolidación automatizada, procesamiento y reportes de los datos recolectados a través del formato HIS.
- Estandarizar todas las diversas versiones anteriores que están siendo usadas en las Diresas, Disas, Redes, Microredes y puntos de digitación.



- Contar con una instalación sin asistencia técnica usando dispositivos magnéticos.
- Enviar, recepcionar y consolidar paquetes de datos desde los establecimientos de salud hasta los demás niveles administrativos, permitiendo alimentar la Base de Datos Central.

### 3.1.2 Características Técnicas

|   |  |
|---|--|
| Plataforma de Desarrollo                      | Lenguaje de programación: Clipper 5.2              |
|   | Sistema de Gestor de Base de Datos: Visual Fox Pro |
|   | Generación de reportes: formato .dbf               |
| Requisitos mínimos para óptimo funcionamiento | Procesador: 386                                    |
|   | Memoria RAM 4 Mb o superior                        |
|   | Espacio libre en Disco Duro: 100Mb o superior      |
|   | Windows XP   |

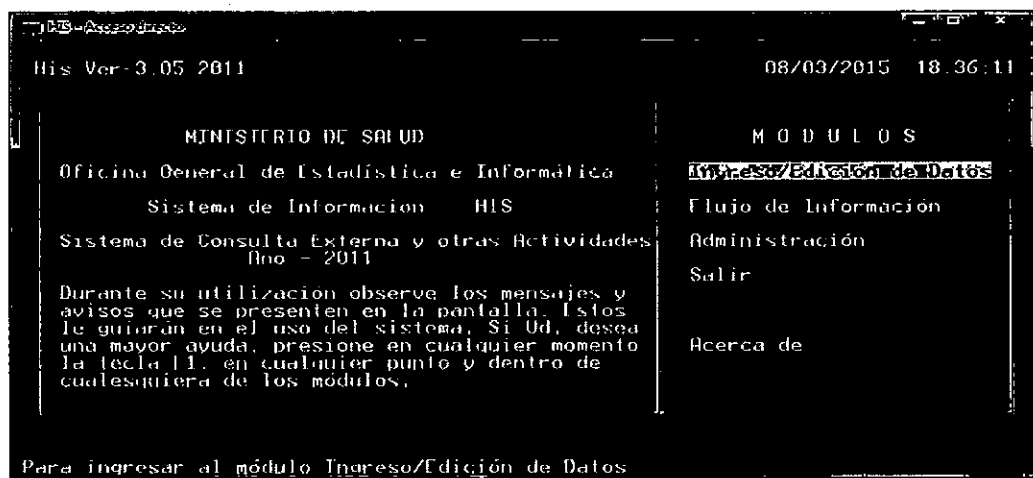
**Tabla N° 8: Características técnicas**

**Fuente: Manual de Instalación del Sistema de Información en Salud**

### 3.1.3 Descripción de los procesos más importantes

#### 3.1.3.1 Proceso de ingreso de datos

En este módulo se realiza el ingreso de producción de cada profesional de la salud, previo ingreso de contraseña. Luego se consigna el código de establecimiento de salud, identificación del lote, número total de páginas, mes y año de los datos, después se procede al ingreso de información.



**Figura N° 3: Ingreso/Edición de datos**

MINISTERIO DE SALUD OFICINA GENERAL DE ESTADISTICA E INFORMATICA  
08/03/2015 18:44:54

NUEVO LOTE

Codigo de FFSS : 200002105 C S MARTA GORETTI / CAST  
Identificación del lote : 002  
Nro. total de Formularios : 10  
Mes y año de los Datos : 01/2015 formato (mm/aaaa)

F1 Ayuda ESC Salir F6 Borrar F7 Regresa F10 Graba F11 Consulta

El archivo del mes y año 01 2015 no existia se ha creado ahora

**Figura N° 4: Ingreso de un nuevo lote**

### 3.1.3.2 Proceso de Edición de datos

En este módulo se realiza la edición de la información ingresada, colocando previamente la contraseña para modificar la información, luego el código de establecimiento de salud, después el número de lote, página a modificar, finalmente año y mes que corresponde.

MINISTERIO DE SALUD OFICINA GENERAL DE ESTADISTICA E INFORMATICA  
08/03/2015 18:50:18

EDICION

Codigo de FFSS : 200002105 C S MARTA GORETTI / CAST  
Identificación del lote : 002  
Nro. de página del lote : 1  
Mes y año de los Datos : 01/2015 formato (mm/aaaa)

F1 Ayuda ESC Salir F6 Borrar F7 Regresa F10 Graba F11 Consulta

El archivo del mes y año 01 2015 no existia se ha creado ahora

**Figura N° 5: Edición de un lote de información digitado**

### 3.1.3.3 Proceso de envío de información

Este proceso consta de realizar el envío de la información digitada durante el mes correspondiente convertido en dos archivos de tipo .DLL. Esos archivos son enviados a la oficina de estadística para hacer la compactación de información de toda la unidad

Ejecutora 400. Previo a esto se debe seleccionar el año y mes a enviar para que se carguen la cantidad de lotes digitados.

HIS - Acceso directo

MINISTERIO DE SALUD OFICINA GENERAL DE ESTADISTICA E INFORMATICA  
08/03/2015 19:04:40

| CODESTAB  | ENVIO ESTABLEC     | ANO  | MES | LTES | PGNAS | RGSTRS |
|-----------|--------------------|------|-----|------|-------|--------|
| 000002105 | C.S. MARIA GORETTI | 2013 | 3   | 7    | 100   | 2711   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 4   | 14   | 180   | 2879   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 5   | 8    | 117   | 10041  |
| 000002105 | C.S. MARIA GORETTI | 2013 | 6   | 12   | 152   | 2413   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 7   | 12   | 155   | 2395   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 8   | 22   | 298   | 3918   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 9   | 19   | 327   | 3929   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 10  | 22   | 335   | 4317   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 11  | 25   | 405   | 5464   |
| 000002105 | C.S. MARIA GORETTI | 2013 | 12  | 16   | 238   | 3355   |
| 000002105 | C.S. MARIA GORETTI | 2014 | 1   | 7    | 118   | 1338   |
| 000002111 | P.S. CRUZ DE CADA  | 2013 | 3   | 1    | 7     | 136    |

F5=Marca/Desmarca 1x1 F8=Marca/Desmarca Todos Enter=Procesar Esc=Salir

Establecimientos con información para enviar al nivel superior

Figura N° 6: Envío de información

### 3.1.3.4 Proceso de recepción de información por lotes

En este proceso se recibe los lotes ingresados en otra computadora para realizar un solo envío a la oficina de informática. Previo a esto se ingresa la letra según la ruta descrita en donde se almacenara la información recepcionada.

HIS - Acceso directo

MINISTERIO DE SALUD OFICINA GENERAL DE ESTADISTICA E INFORMATICA  
08/03/2015 19:09:41

RECEPCION DE INFORMACION

Dispositivo desde donde se Recepcionara  
D = DISKETTE  
H = DISCO DURO (Ruta = \His\hisv4\Hisrecep)

Figura N°7: Recepción de información

### 3.1.3.5 Proceso de creación de clave de digitador

En este proceso se crea la clave de acceso para cada digitador, con la finalidad de que cada uno se haga responsable de la información que digita, para una posterior corrección si el caso lo amerita, esto por lo general cuando se desea realizar un control de calidad a la información de las diferentes estrategias sanitarias.

The screenshot shows a window titled 'MIS Acceso directo'. Inside, the header reads 'MINISTERIO DE SALUD' on the left and 'OFICINA GENERAL DE ESTADISTICA E INFORMATICA' on the right, with a date and time '08/03/2015 19:18:37' on the far right. The main title of the form is 'INGRESO DE DIGITADORES'. Below this, there are three input fields: 'Nombre del Digitador' with the text 'CARMEN RAMOS ARCA' entered, 'Clave' with asterisks '\*\*\*\*\*', and 'Confirmar Clave' with asterisks '\*\*\*\*\*'. At the bottom of the form area, there is a legend: 'F1=Ayuda ESC=Sale F10=Acepta F11=Consulta'. At the very bottom of the window, a status bar says 'Confirme la clave que tendrá el Digitador'.

**Figura N° 8: Creación de la clave para digitar**

### 3.1.3.6 Proceso de mantenimiento de Personal

En este proceso se ingresa al personal que es nuevo en cada establecimiento de salud, para luego realizar los reportes de la producción para evaluar el nivel de rendimiento de cada uno.

```

HIS - Acceso directo
MINISTERIO DE SALUD                                OFICINA GENERAL DE ESTADISTICA E INFORMATICA
                                                    08/03/2015  21:47:36

MANTENIMIENTO DE PERSONAL
CodPsal : 
Nombre : 
Plaza : 
Establecimiento : 
Profesión u Ocupación : 
Condición : 
Fecha de Ingreso : 
Fecha de Baja : 

F1=Ayuda ESC=Sale F5=Elim. F7=Regresa F10=Graba F11=Consulta
F12=tabla de Colegios

Ingrese elCodigo de Personal
  
```

**Figura N° 9: Mantenimiento de personal**

## **3.2 Descripción del Aplicativo para el Registro de Formatos SIS**

### **3.2.1 Descripción General**

El ARFSIS ha sido desarrollado por la Oficina de Informática y Estadística del SIS Central, con la colaboración de los Responsables de Informática de las Oficinas Desconcentradas del SIS. Registra las atenciones de los asegurados SIS en todos los tipos de seguros (SIS INDEPENDIENTE, SIS NRUS, SIS EMPRENDEDOR, SIS GRATUITO), así mismo brinda reportes según la necesidad del gerente, además está conectado con el sistema de RENIEC para los datos de los pacientes.

### 3.2.2 Características Técnicas

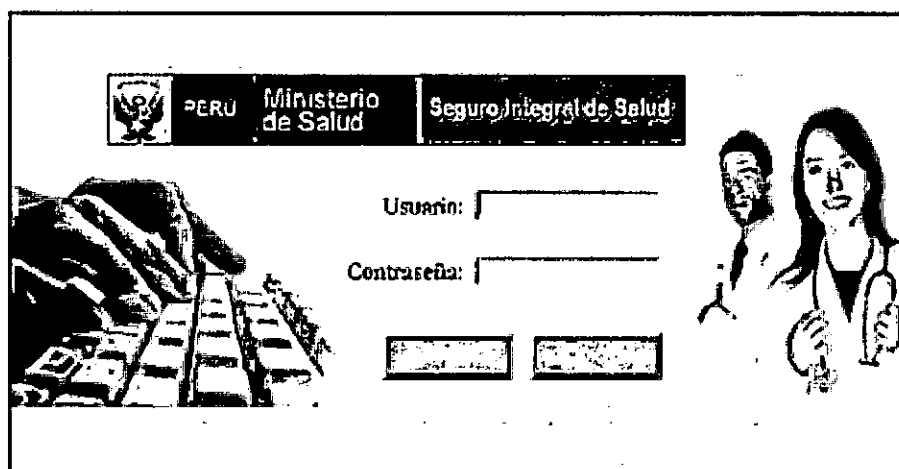
|  |   |
|--|---|
| <b>Plataforma de Desarrollo</b>                          | Lenguaje de Programación: Visual Basic 6.0              |
|  | Sistema Gestor de BD: MySQL 5.0                         |
|  | Controlador ODBC: ODBC/MYSQL 5.1                        |
|  | Compresión de Paquete de Envío: Dynazip                 |
|  | Generación Reportes: Formato .xls                       |
| <b>Sistemas Integrados</b>                               | ARFSIS  |
|  | Seguridad   |
| <b>Requerimientos Mínimos para óptimo funcionamiento</b> | Procesador: Pentium IV 3.0 Ghz, similar o superior      |
|  | Memoria RAM 1 GB o superior                             |
|  | Espacio Libre en Disco Duro: 2 Gb o superior            |
|  | Tarjeta de red y Switch: 10/100/1000                    |
|  | Monitor 15" con resolución mínima de 1024*768           |
|  | Cableado UTP Cat 5E                                     |
|  | Windows XP SP3 o superior                               |
| <b>Funcionalidad</b>                                     | Entorno amigable, intuitivo, rápido, seguridad de datos |

**Figura N° 10: Características técnicas del Aplicativo de Registro de Formatos SIS**

### 3.2.3 Descripción de los procesos

#### 3.2.3.1 Acceso al aplicativo

Ejecutar el acceso directo al Aplicativo ARFSIS.exe, lo cual nos llevará al Formulario de Acceso e Identificación de Usuario.



**Figura N° 11: Ingreso al Aplicativo de Registro de Formatos SIS**

Es obligatorio que cada personal responsable de digitación cuente y haga uso de su propia clave de acceso, la cual es personal e intransferible. El Administrador del Centro de Cómputo del Punto de Digitación es el encargado de la creación de las cuentas de usuario y contraseñas, asimismo de asignar los accesos a las estaciones de trabajo del Punto de Digitación y del mantenimiento de la información que se registra por medio del ARFSIS, quedando bajo su responsabilidad dichos procesos.

### **3.2.3.2 Registro de Formatos Únicos de Atención**

En este módulo se hace el ingreso de cada ficha de atención, ingresando previamente el código de cada ficha, el cual es único e irrepetible, posterior a eso se ingresa el DNI del paciente para luego llenar los datos correspondientes en la atención médica como lo es el diagnóstico, medicamentos y procedimientos realizados.





### 3.2.3.4 Backup de base de datos

Se debería sacar copias de la información a diario, y este proceso hace posible eso, guardando el backup en el disco duro de la computadora.

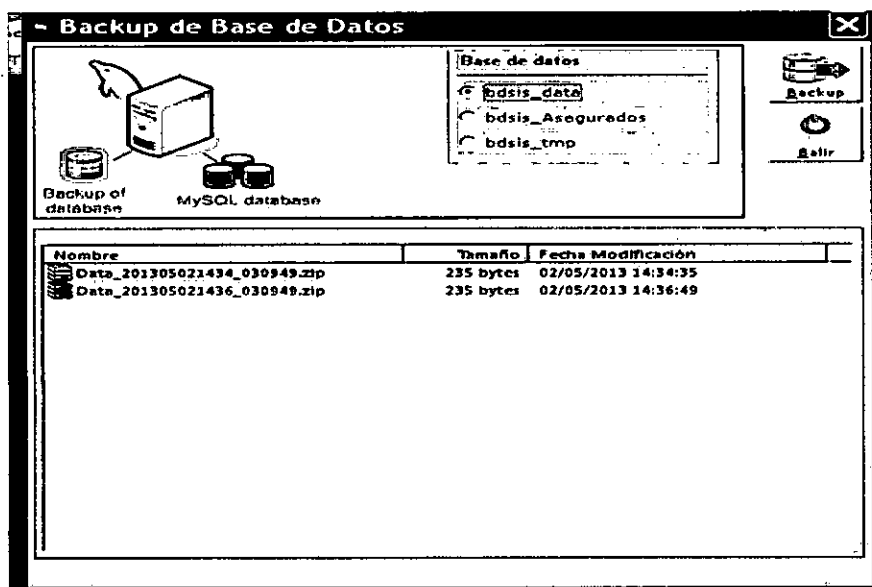


Figura N° 14: Buckup de base de datos

### 3.2.3.5 Restaurar base de datos

Este proceso implica restaurar un backup de toda la información ingresada durante el mes, además se restaura la base de datos de asegurados que el SIS envía mensualmente a cada establecimiento de salud, como también la base de datos maestro en la que contiene toda la información de cada profesional de la salud.

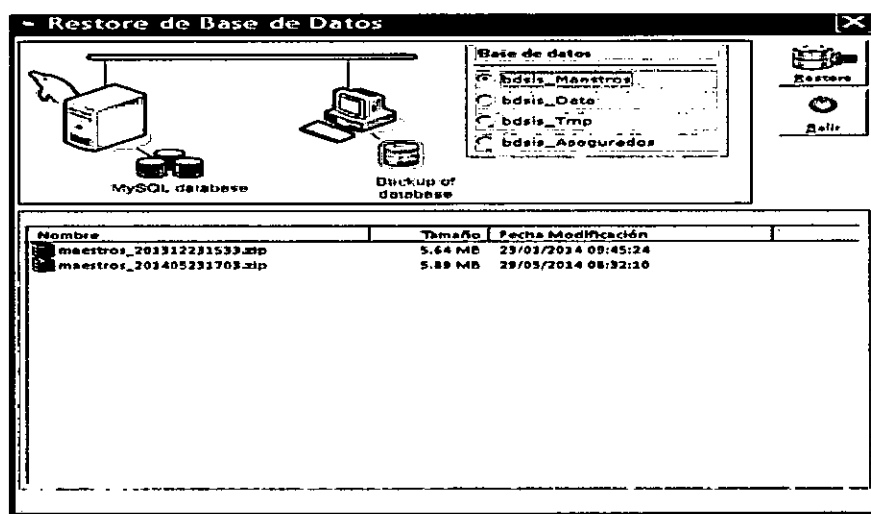


Figura N° 15: Restaurar base de datos

### 3.2.3.6 Envío de información

Este proceso consiste en sacar un backup de la base de datos, luego realizar un control de calidad previo antes de realizar el envío de información, después se hace click en envío y posterior a eso se realiza el último control de calidad para observar fichas rechazadas por reglas de consistencia, y finalmente se culmina el proceso de exportación de información.

**Envío de Información**

Periodo de Proceso: MARZO 2015      Paquete de Envío: 01

Ruta y nombre del archivo de envío: C:\Archivos de programa\Seguro Integral de

**PROCESO DE EXPORTACION DE INFORMACION**

Exportando Tablas Transaccionales

|   |   |
|---|---|
| <input type="checkbox"/> Fese             | <input type="checkbox"/> Atenciones             |
| <input type="checkbox"/> F. Integrantes   | <input type="checkbox"/> Serv. Materno Infantil |
| <input type="checkbox"/> Revocatoria Fese | <input type="checkbox"/> Diagnóstico            |
| <input type="checkbox"/> Inscripciones    | <input type="checkbox"/> Medicamentos           |
| <input type="checkbox"/> Afilaciones      | <input type="checkbox"/> Insumos                |
| <input type="checkbox"/> No Asegurados    | <input type="checkbox"/> Procedimientos         |
| <input type="checkbox"/> Actualizaciones  | <input type="checkbox"/> Usuarios de Sistema    |
| <input type="checkbox"/> Anulación        |   |
| <input type="checkbox"/> Resp. Aplicación |   |

☐ Empaquetado Archivo      ☐ Proceso Terminado

Envío    Anular Envío    Backup    QC    Salir

Figura N° 16: Envío de información del Aplicativo

### 3.2.3.7 Cierre de periodo

Este proceso permite realizar el cierre del periodo por mes, con la finalidad que permita ingresar fichas del mes siguiente y además imposibilita el ingreso de fichas atrasadas ya sea por cualquier motivo. Esto se realiza después de realizar el envío correspondiente de la base de datos la cual contiene las atenciones realizadas en cada establecimiento de salud.

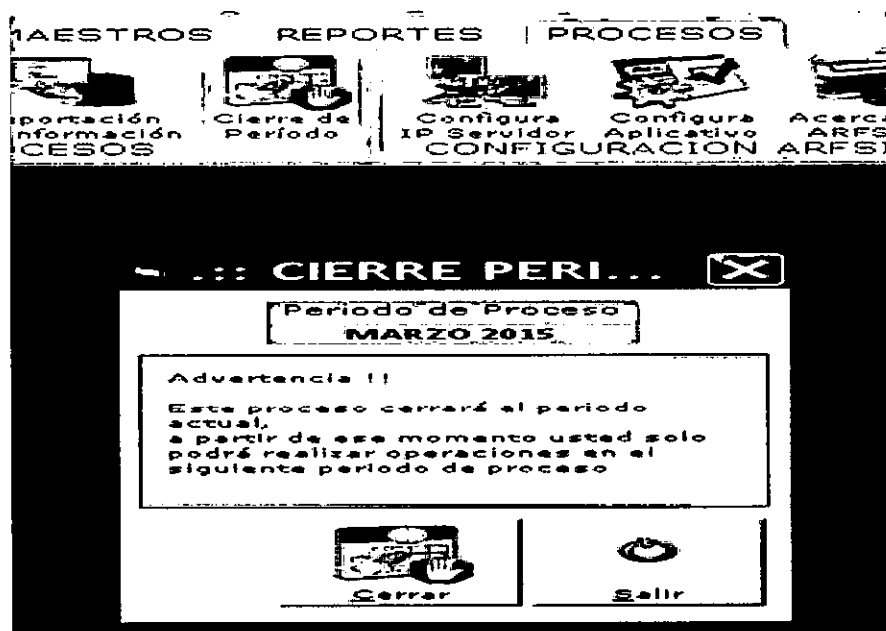


Figura N° 17: Cierre de periodo

### 3.2.3.8 Configuración del aplicativo

La configuración del aplicativo se realiza por cada establecimiento de salud, seleccionando el modo de trabajo, es decir si se desea trabajar con la base de datos del establecimiento y la base de datos del SIS, o si se desea trabajar conectados a internet o quizás el establecimiento de salud no cuenta con internet se trabajará con la opción fuera de línea.

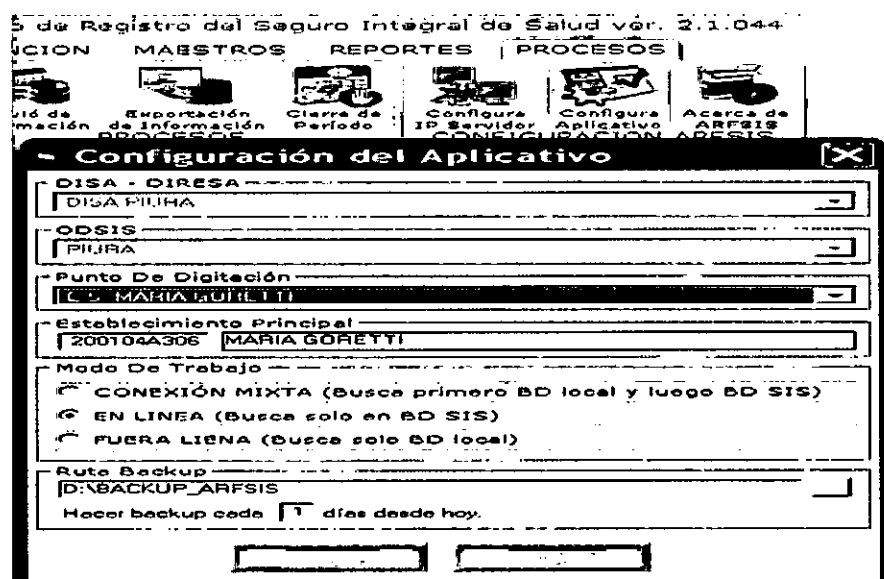


Figura N° 18: Configuración de aplicativo

### 3.3 Evaluación de riesgos

Se tomará en cuenta la Guía de Control Interno para realizar la evaluación de riesgos.

#### 3.3.1 Identificación de riesgos

##### 3.3.1.1 Técnica de recopilación de información

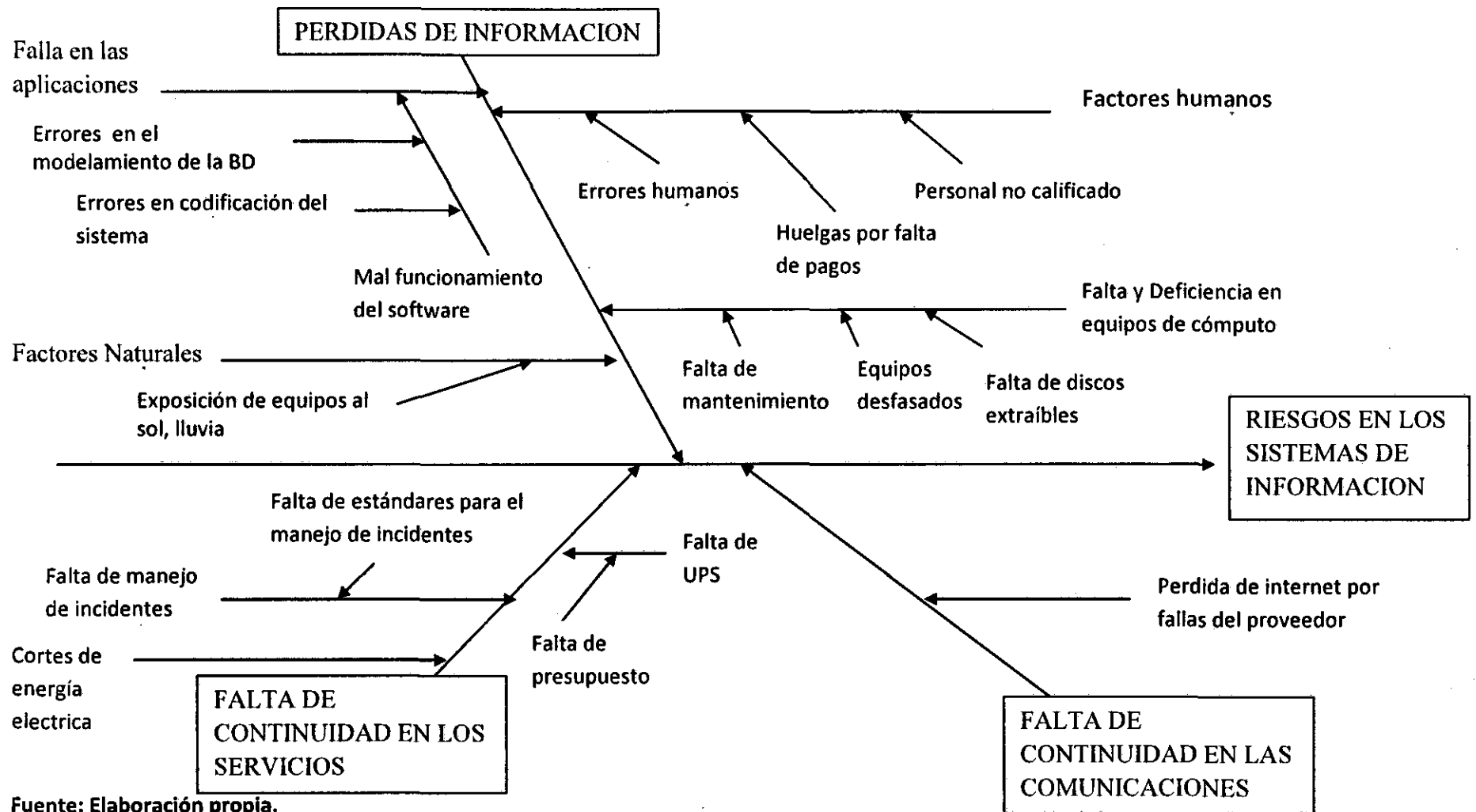
Se realizó una entrevista al jefe del área de informática de la Dirección Regional de Salud Piura, el Sr Segundo Livia García, quien proporcionó información para realizar la matriz FODA mostrada a continuación.

| <b>FORTALEZAS</b>   | <b>OPORTUNIDADES</b>   |
|---|--|
| <ul style="list-style-type: none"><li>1.- Mantenimiento a los sistemas por la oficina central de informática en el momento que se requiera.</li><li>2.- Capacitaciones permanentes para el manejo de los sistemas de acuerdo a actualizaciones.</li><li>3.- Actualización permanente de cada sistema.</li><li>4.- Apoyo por parte de la oficina de informática de la Dirección Regional de Salud Piura en el desarrollo de proyectos para la mejora de la gestión de la información.</li><li>5.- Cada sistema cuenta con el manual de instalación y usuario de los sistemas.</li></ul>      | <ul style="list-style-type: none"><li>1.- La gran parte de la población acude a los establecimientos de salud para acceder a los servicios básicos, y de esta forma hay buenos datos para procesar.</li><li>2.- Innovación científico - tecnológica.</li></ul>   |
| <b>DEBILIDADES</b>  | <b>AMENAZAS</b>  |
| <ul style="list-style-type: none"><li>1.- Falta de apoyo por parte de la Dirección Regional de Salud para la contratación de personal calificado para el ingreso de información y administración de base de datos.</li><li>2.- No todos los establecimientos de salud cuenta con internet.</li><li>3.- Los antivirus no están actualizados y no son originales.</li><li>4.- El sistema de información en Salud solo se ejecuta en su totalidad con el Sistema Operativo Windows XP.</li><li>5.- Los establecimientos no tienen discos extraíbles de gran capacidad para almacenar</li></ul> | <ul style="list-style-type: none"><li>1.-Falla en la continuidad del fluido eléctrico.</li><li>2.- Recorte presupuestal por parte del Ministerio de Economía y Finanzas al Seguro Integral de Salud, lo que ocasiona la falta de equipos de cómputo y otros materiales.</li><li>3.- Exposición de equipos de cómputo al medio ambiente (rayos solares, polvo, lluvia).</li><li>6.- Ocasionalmente falta de servicio de</li></ul> |

|  |   |
|--|---|
| <p>la información.</p> <p>6.- Falta de mantenimiento al equipo de cómputo.</p> <p>7.- Deficiencia en el diseño y codificación del Sistema de Información en Salud.</p> <p>8.- Actualizaciones manuales.</p> <p>9.- Entrega de información fuera de plazo para ser ingresada en las fechas establecidas en cada establecimiento de salud.</p> <p>10.- Falta de una arquitectura adecuada para la seguridad de la información.</p> | <p>internet por fallas del proveedor.</p> <p>7.- Falta de pagos salariales al personal que digita la información, teniendo como consecuencia huelgas.</p> |
|--|---|

**Tabla N° 8: Análisis FODA de los sistemas de información.**  
**Fuente: Elaboración propia**

### 3.3.1.2 Técnica de diagramación



Fuente: Elaboración propia.

### 3.3.1.3 Registro de riesgo

| Sistema de Información en Salud y Aplicativo para el Registro de Formatos SIS |  |                     |  |   |
|---|--|---------------------|--|---|
| Riesgo  |  | Tipo de riesgo      | Causas(factoros internos y externos)   | Efectos/Consecuencias   |
| R1  | Contratación de personal no calificado           | Riesgo operativo    | <ul style="list-style-type: none"> <li>Falta de compromiso por parte de la DIRESA Piura en realizar una rigurosa selección de personal.</li> <li>En los establecimientos de salud se contrata a personal que muchas veces no cumplen con los requisitos deseados.</li> </ul> | <ul style="list-style-type: none"> <li>Desconocimiento del uso del gestor de base de datos.</li> <li>No existe un manejo eficiente de los sistemas de información.</li> <li>Errores humanos con frecuencia.</li> <li>Perdida de información.</li> </ul> |
| R2  | Corte de fluido eléctrico                        | Riesgo de operativo | <ul style="list-style-type: none"> <li>Falta de pago del servicio.</li> <li>Falta de UPS.</li> </ul>   | <ul style="list-style-type: none"> <li>Perdida de información cuando la computadora se apaga de forma no adecuada.</li> <li>Falla en los sistemas, a tal punto que después del corte de energía no se pueden ejecutar los sistemas.</li> </ul>          |
| R3  | Falta de presupuesto al Seguro Integral de Salud | Riesgo Financiero   | <ul style="list-style-type: none"> <li>No cumplimiento de las metas programadas por cada indicador prestacional del SIS.</li> <li>Malversaciones del presupuesto.</li> </ul>   | <ul style="list-style-type: none"> <li>Perdida de dinero por incumplimiento de las metas programadas.</li> <li>Desabastecimiento en equipos de cómputo modernos, material de escritorio, pagos de servicios, etc.</li> </ul>                            |

| Riesgo |  | Tipo de riesgo       | Causas(factoros internos y externos)   | Efectos/Consecuencias  |
|--------|--|----------------------|--|--|
| R4     | Falta de Recursos Directamente Recaudados en los establecimientos de salud | Riesgo Financiero    | <ul style="list-style-type: none"> <li>• La mayoría de atenciones son por el Seguro Integral de Salud las cuales son gratuitas, y hay pocas atenciones pagadas de pacientes particulares.</li> </ul> | <ul style="list-style-type: none"> <li>• Desabastecimiento en los servicios básicos de salud.</li> <li>• Pagos a destiempo de los trabajadores, es decir no se les paga de forma mensual.</li> <li>• Falta de mantenimiento de equipos por falta de dinero.</li> <li>• Falta de equipos como por ejemplo discos extraíbles para guardar información.</li> <li>• Huelgas por falta de pagos.</li> </ul> |
| R5     | Exposición de equipos de cómputo al medio ambiente                         | Riesgo de tecnología | <ul style="list-style-type: none"> <li>• Ubicación incorrecta de los equipos.</li> <li>• Falta de cortinas.</li> <li>• Oficinas poco espaciosas.</li> </ul>  | <ul style="list-style-type: none"> <li>• Deterioro de los equipos con facilidad.</li> <li>• Perdida de la información porque los equipos de malogran.</li> <li>• Ambiente no adecuado para trabajar.</li> </ul>  |
| R6     | Falta de internet  | Riesgo de tecnología | <ul style="list-style-type: none"> <li>• Falta de pago oportuno por el servicio.</li> <li>• Falla en el servicio brindado por la empresa proveedora.</li> </ul>                                      | <ul style="list-style-type: none"> <li>• Interrupción en la digitación de información.</li> <li>• Fichas acumuladas y enviadas de forma inoportuna al nivel central.</li> </ul>  |



|    |                           |                  |   |  |
|----|---------------------------|------------------|---|--|
| R7 | Falla en las aplicaciones | Riesgo operativo | <ul style="list-style-type: none"> <li>• Errores en el modelamiento de las bases de datos.</li> <li>• Errores en la codificación y validación del sistema de información en Salud.</li> </ul> | <ul style="list-style-type: none"> <li>• Pérdida de información.</li> <li>• Más de una persona usa el mismo usuario y contraseña para digitar al mismo tiempo.</li> <li>• No hay información clara sobre el responsable de digitación de cada ficha en caso de auditoría.</li> </ul> |
|----|---------------------------|------------------|---|--|

**Tabla N° 9: Matriz de registro de riesgos.**

**Fuente: Anexo N° 2**

### 3.3.2 Valoración de riesgos

En la valoración de riesgos se tomará en cuenta la Tabla N° 9 para poder determinar el nivel de riesgo y las acciones que se pueden tomar a nivel de unidad ejecutora en la región Piura.

Se realizará una escala de medida cualitativa a continuación:

| <b>Categoría</b>  | <b>Definición</b>   |
|-------------------|---|
| <b>PROBABLE</b>   | Es muy frecuente la materialización del riesgo o se presume que llegara a materializarse en los establecimientos de salud de la unidad ejecutora 400. |
| <b>POSIBLE</b>    | Es frecuente la materialización del riesgo o se presume que posiblemente se podrá materializar establecimientos de salud de la unidad ejecutora 400.  |
| <b>IMPROBABLE</b> | Es poco frecuente la materialización del riesgo o se presume que no llegara a materializarse establecimientos de salud de la unidad ejecutora 400.    |

**Tabla N° 10: Escala de medida cualitativa de la probabilidad.**  
**Fuente: Guía de control interno (2008)**

Ese mismo diseño se adapta al tema de estudio, estableciendo las categorías y la descripción, tal como se muestra a continuación.

| <b>Categoría</b>  | <b>Definición</b>  |
|-------------------|--|
| <b>DESASTROSO</b> | Si el hecho llegara a presentarse, tendrá alto impacto o efecto sobre la gestión en los establecimientos de salud de la unidad ejecutora 400.  |
| <b>MODERADO</b>   | Si el hecho llegara a presentarse, tendrá medio impacto o efecto sobre la gestión en los establecimientos de salud de la unidad ejecutora 400. |
| <b>LEVE</b>       | Si el hecho llegara a presentarse, tendrá bajo impacto o efecto sobre la gestión en los establecimientos de salud de la unidad ejecutora 400.  |

**Tabla N° 11: Escala de medida cualitativa del impacto.**  
**Fuente: Guía de control interno (2008)**

### **3.3.3 Matriz de riesgos**

Constituye una herramienta metodológica que permite hacer un inventario de riesgos sistemáticamente agrupados por clase o tipo de riesgo y ordenado prioritariamente de acuerdo con el nivel de riesgos. En este mapa se describen los riesgos identificados y se justifica el nivel de cada uno de ellos en la Unidad Ejecutora 400.

| Riesgo |  | Evaluación del riesgo |       |            |       |                 |       | Respuesta al Riesgo |  |  | Riesgo residual | Responsa ble         |
|--------|--|-----------------------|-------|------------|-------|-----------------|-------|---------------------|--|--|-----------------|----------------------|
|        |  | Probabilidad          |       | Impacto    |       | Nivel de Riesgo |       |                     |  |  |                 |                      |
|        |  | Nivel                 | Valor | Nivel      | Valor | Nivel           | Valor | Respuesta           | Actividades  | Controles necesarios   |                 |                      |
| R1     | Contratación de personal no calificado           | Posible               | 2     | Desastroso | 3     | Importante      | 6     | Reducir             | Establecer perfiles necesarios para la contratación de personal. | <ul style="list-style-type: none"><li>• Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleos.</li><li>• Exigir capacitación en manejo del gestor de base de datos SQL SERVER.</li><li>• Realizar una inducción previa de los procesos que se anejan en cada sistema.</li></ul> | Moderado        | Oficina de RRHH      |
| R2     | Corte de fluido eléctrico                        | Posible               | 2     | Desastroso | 3     | Importante      | 6     | Reducir             | Realizar la compra de UPS para las computadoras                  | <ul style="list-style-type: none"><li>• Equipar las computadoras para protegerlas de fallas de energía y de otras anomalías eléctricas por fallo en el suministro eléctrico.</li><li>• Practicar estándares para el manejo de este tipo de incidentes.</li></ul>   | Moderado        | Oficina de logística |
| R3     | Falta de presupuesto al Seguro Integral de Salud | Posible               | 2     | Moderado   | 2     | Moderado        | 4     | Evitar              | Realizar auditorías permanentes a la información digitada.       | <ul style="list-style-type: none"><li>• Se planificaran cuidadosamente las auditorías de los sistemas a fin de minimizar el riesgo de interrupciones a los procesos de negocio.</li></ul>  |                 | Oficina del SIS      |

|    |   |          |   |            |   |             |   |            |  |   |            |   |
|----|---|----------|---|------------|---|-------------|---|------------|--|---|------------|---|
|    |   |          |   |            |   |             |   |            |  | <ul style="list-style-type: none"> <li>• Cumplir con el levantamiento de observaciones en la auditoria.</li> </ul>  |            |   |
| R4 | Falta de Recursos Directamente Recaudados(RDR) en los establecimientos de salud | Probable | 3 | Desastroso | 3 | Inaceptable | 9 | Reducir    | Elaborar estrategias para generar ingresos económicos a los establecimientos de salud. | <ul style="list-style-type: none"> <li>• Debe existir una buena gestión para la administración de los recursos.</li> <li>• Brindar servicios especializados por convenio para recaudar fondos RDR.</li> </ul>   | Importante | Gerencias                                 |
| R5 | Exposición de equipos de cómputo al medio ambiente                              | Posible  | 2 | Moderado   | 2 | Moderado    | 4 | Reducir    | Coordinar el mejoramiento de condiciones para proteger a los equipos.                  | <ul style="list-style-type: none"> <li>• Se debe designar y mantener protección física contra daños por rayos solares, fuego, inundación, etc.</li> <li>• El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidades de acceso no autorizado.</li> <li>• Los equipos recibirán un adecuado mantenimiento cada cierto tiempo de forma periódica.</li> </ul> |            | Jefatura de cada establecimiento de salud |
| R6 | Falta de internet   | Posible  | 2 | Desastroso | 3 | Importante  | 6 | Transferir | Informar al proveedor de las fallas detectadas.  | <ul style="list-style-type: none"> <li>• Cambiar de proveedor</li> </ul>  | Moderado   | Proveedor de internet                     |
| R7 | Falla en las aplicaciones   | Probable | 3 | Desastroso | 3 | Inaceptable | 9 | Reducir    | Informar a la oficina de informática de  | <ul style="list-style-type: none"> <li>• Se validara el ingreso de datos a los sistemas de aplicación para asegurar</li> </ul>  | Importante | Oficina de informatic                     |

|  |  |  |  |  |  |  |  |  |                               |   |  |   |
|--|--|--|--|--|--|--|--|--|-------------------------------|---|--|---|
|  |  |  |  |  |  |  |  |  | las deficiencias encontradas. | que sean correctos y adecuados.<br>• Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información. |  | a |
|--|--|--|--|--|--|--|--|--|-------------------------------|---|--|---|

**Tabla N° 12: Matriz de riesgos**  
**Fuente: Guía de Control Interno (2008)**

### 3.3.4 Matriz de situación de riesgo residual

| Probabilidad |   |      |              |                                   |
|--------------|---|------|--------------|-----------------------------------|
| Probable     | 3 |      |              | R4 R7<br>↓ ↓                      |
| Posible      | 2 |      | R3 R5<br>↓ ↓ | R4 R7<br>↓ ↓<br>R1 R2 R6<br>↓ ↓ ↓ |
| Improbable   | 1 |      |              | R1 R2 R6<br>↓ ↓ ↓                 |
| Impacto      |   | 1    | 2            | 3                                 |
|              |   | Leve | Moderado     | Catastrófico                      |

Tabla N° 13: Matriz residual

Fuente: Guía de Control Interno

Esta matriz de riesgo residual implica que los riesgos R3 Y R4 necesitan monitorización, planes de actuación detectivos o pueden ser aceptados por la entidad. El riesgo R1, R2 y R6 necesitan investigar planes de actuación preventiva. Finalmente los riesgos R4 Y R7 necesitan mitigación de riesgos, es decir hay que tomar medidas correctivas.

## **CAPÍTULO 4: PROPUESTA DE UN PLAN DE AUDITORIA INFORMÁTICA**

### **4.1 Alcance de la propuesta del plan de auditoría informática**

El alcance de la propuesta de un plan de auditoría informática consta de los siguientes objetivos:

- Evaluar la base de datos del Sistema de Información en Salud y la del Aplicativo para el Registro de Formatos SIS.
- Comprobar si existe algún plan de mitigación de riesgos frente a los inconvenientes presentados al momento de ejecutar cada sistema de información.
- Verificar que los sistemas cuenten con los equipos e infraestructura adecuada para su eficiente y eficaz funcionamiento.

### **4.2 Criterios a aplicar de la propuesta del plan de auditoría informática**

La propuesta del plan de auditoría informática se realizará en base a lo siguiente:

- NTP/ISO IEC 27001:2008
- NTP/ISO IEC 17799:2007
- Guía para la Implementación del Sistema de Control Interno de las Entidades del Estado Peruano.
- Normas de Auditoría Gubernamental
- Manual de Auditoría gubernamental
- ISO 22301:2012
- Resolución Ministerial 129-2012-PCM
- Manual de Organización y Funciones de la Dirección Regional de Salud Piura.
- POI de la Dirección Regional de Salud Piura
- Resolución Jefatural N° 170 / SIS

### **4.3 Definición de objetivos de control**

#### **4.3.1 Objetivos de control para la evaluación de la Seguridad en Recursos Humanos**

- Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.



- Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.

#### **4.3.2 Objetivos de control para la evaluación de la seguridad física**

- Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio, aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.
- Verificar la prevención de pérdidas y daños en los activos, equipos e infraestructura adecuada, así como la interrupción de las actividades en el establecimiento de salud.

#### **4.3.3 Objetivos de control para la evaluación de la gestión de comunicaciones y operaciones**

- Verificar la operación correcta y segura de los recursos de procesamiento de información.
- Verificar el mantenimiento apropiado de la seguridad y recepción de la información en concordancia con los acuerdos tomados en la entrega de producción por parte del profesional de la salud.
- Verificar la integridad y disponibilidad del procesamiento de información y servicios de comunicación.

#### **4.3.4 Objetivos de control para la evaluación del control de accesos a los sistemas de información**

- Verificar que el acceso de usuario es autorizado de acuerdo a los perfiles de los sistemas de información.
- Verificar la existencia de perfiles de usuario en los sistemas de información.

#### **4.3.5 Objetivos de control para la gestión de incidentes en la seguridad de la información**

- Verificar que las debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de manera tal que permitan tomar acciones correctivas a tiempo.

#### **4.3.6 Objetivos de control para la evaluación de cumplimiento de normas**

- Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.
- Verificar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.

#### **4.3.7 Objetivos de control para la evaluación de base de datos, archivos y datos**

- Verificar que la información almacenada en las bases de datos es de gran valor para la entidad, y esté protegida contra su pérdida o robo.
- Identificar las medidas de seguridad empleadas para conservar correctos los datos en la base de datos, con el fin de mantener su integridad.

### **4.4 Procedimientos de Auditoria**

Se realizará los procedimientos de acuerdo a cada objetivo de control.

#### **Objetivo N° 1:**

Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.

Procedimientos de auditoria:

1. Solicitar al área de recursos humanos de cada establecimiento de salud el curriculum vitae documentado de cada trabajador que administrará la base de datos de cada sistema de información.
2. Comprobar los antecedentes consignados en el curriculum vitae como las certificaciones académicas y profesionales, comprobación de identificación.

3. Verificar la firma del contrato de empleo, como también el documento firmado de confidencialidad y no divulgación de la información que se administrará.

**Objetivo N° 2:**

Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.

Procedimientos de auditoria:

1. Solicitar el documento o guía donde está explícito la relación de responsabilidades asignadas a los trabajadores del área de estadística e informática según los roles de seguridad de información en cada establecimiento de salud.
2. Verificar que el trabajador del área de estadística e informática ha recibido una inducción previa sobre el trabajo a realizar en los diferentes establecimientos de salud.
3. Verificar si existe alguna documentación sobre el proceso formal disciplinario para empleados que han cometido alguna falta con respecto a la seguridad de la información.

**Objetivo N° 3:**

Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio, aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.

Procedimientos de auditoria:

1. Verificar si existe un plan de contingencia en la oficina de estadística e informática.
2. Verificar si el plan de contingencia se ejecuta cuando es necesario.

#### **Objetivo N° 4:**

Verificar la prevención de pérdidas y daños en los activos, equipos e infraestructura adecuada, así como la interrupción de las actividades en el establecimiento de salud.

Procedimientos de auditoria:

1. Verificar que la posición de los equipos minimicen el acceso innecesario a las áreas de trabajo, es decir que las personas no autorizadas tenga acceso.
2. Verificar si los establecimientos de salud cuentan con alguna política de seguridad sobre la prohibición de fumar, beber y comer cerca de los equipos que procesan información.
3. Verificar si la oficina de estadística e informática de los establecimientos de salud cuentan con equipos y tecnología (software, cableado y servidores) adecuados para un funcionamiento continuo de los equipos que procesen todo tipo de información.
4. Verificar que cuenten con generador de respaldo en funcionamiento cuando se prolongue la falta de energía eléctrica.
5. Verificar si cuentan con luces de emergencia y que se encuentren en funcionamiento.
6. Verificar la correcta instalación de forma separada del cableado de energía como el cableado de telecomunicaciones.
7. Solicitar la documentación necesaria sobre la cantidad de fallas en los equipos, como las correcciones preventivas y correctivas, además de eso el periodo de tiempo en el que se realiza el mantenimiento a los equipos.
8. Verificar antes de la baja de equipos los datos importantes y software con licencias.
9. Verificar si existe algún registro de autorización sobre la salida de equipos fuera de los establecimientos de salud.

#### **Objetivo N° 5:**

Verificar la operación correcta y segura de los recursos de procesamiento de información

Procedimientos de auditoria:

1. Verificar si los digitadores tienen la documentación sobre los procedimientos de operación como por ejemplo los procedimientos de prendido y apagado, backups, mantenimiento de equipos, ambientes de cómputo y manipulación de correos.
2. Verificar la existencia de documentación sobre procedimientos formales de gestión para asegurar un control de todos los cambios en los equipos y el software.
3. Solicitar documentación sobre la segregación de funciones en el área de estadística e informática de los establecimientos de salud.

**Objetivo N° 6:**

Verificar el mantenimiento apropiado de la seguridad y recepción de la información en concordancia con los acuerdos tomados en la entrega de producción por parte del profesional de la salud.

Procedimientos de auditoria:

1. Solicitar la documentación donde hace constar los plazos de entrega de información por parte de los profesionales de la salud.
2. Solicitar los informes de las auditorías realizadas a la información por las diferentes oficinas del nivel central.

**Objetivo N° 7:**

Verificar la integridad y disponibilidad del procesamiento de información y servicios de comunicación.

Procedimientos de auditoria:

1. Solicitar las políticas de extracción de buckups de los sistemas de información, así mismo verificar que las copias de seguridad de la información estén guardadas en una locación remota, como por ejemplo discos extraíbles.

**Objetivo N° 8:**

Verificar que el acceso de usuario es autorizado de acuerdo a los perfiles de los sistemas de información.

Procedimientos de auditoria:

1. Solicitar la documentación del control de acceso de cada usuario a los sistemas de información especificando además de los cambios, el pedido de acceso, autorización de acceso y administración de accesos.

**Objetivo N° 9:**

Verificar la existencia de perfiles de usuario en los sistemas de información.

Procedimientos de auditoria:

1. Solicitar la documentación de los perfiles de usuarios de los sistemas de información.
2. Solicitar la documentación de la asignación de contraseñas a los usuarios de los sistemas.

**Objetivo N° 10:**

Verificar que las debilidades en la seguridad de información asociados con los sistemas de información sean comunicadas de manera tal que permitan tomar acciones correctivas a tiempo.

Procedimientos de auditoria:

1. Solicitar el reporte de eventos sobre la pérdida de la seguridad de la información como por ejemplo fallas en los sistemas, errores humanos o pérdida de equipos.
2. Verificar el reporte inmediato de los eventos a una instancia superior por parte de los trabajadores del área de estadística e informática.

**Objetivo N° 11:**

Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.

**Procedimientos de auditoria:**

1. Solicitar la planificación de las posibles auditorias por parte del encargado del área de informática.
2. Solicitar todos los registros de auditoria ejecutadas a los sistemas por parte de un nivel superior.
3. Verificar si existe el seguimiento de las recomendaciones dejadas en las supervisiones.

**Objetivo N° 12:**

Verificar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.

**Procedimiento de auditoria:**

1. Verificar que los sistemas cumplan con las políticas y estándares de seguridad de los establecimientos de salud.

**Objetivo N° 13:**

Verificar que la información almacenada en las bases de datos es de gran valor para la entidad, y esté protegida contra su pérdida o robo.

**Procedimiento de auditoria:**

1. Solicitar las metas programadas en los años 2013, 2014 y 2015 de cada establecimiento de salud para evaluar su cumplimiento según la información.
2. Verificar si existe algún incentivo o premio por cumplimiento de las metas programadas basadas en la información de cada sistema informático.

**Objetivo N° 14:**

Identificar las medidas de seguridad empleadas para conservar correctos los datos en la base de datos, con el fin de mantener su integridad.

1. Verificar que existen medidas de seguridad para conservar la integridad de los datos almacenados en cada sistema de información.

#### 4.5 Programa de auditoria a aplicar

##### PROGRAMA DETALLADO DE AUDITORIA

**Nombre de la Entidad: DIRECCION REGIONAL DE SALUD PIURA - ESTABLECIMIENTOS DE SALUD DE LA UNIDAD EJECUTORA 400.**

**Fecha de auditoría :** .....

| PROGRAMADO |     | AREA DE INFORMATICA  | TERMINADO  |              |     |
|------------|-----|--|------------|--------------|-----|
| NOMBRE     | H/S |  | Ref.<br>PT | Hecho<br>por | H/S |
|            |     | <b>Objetivo N° 1:</b><br>Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.<br><b>Criterio:</b> <ul style="list-style-type: none"> <li>- Reglamento de Organización y Funciones (ROF).</li> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 - 2008</li> </ul> <b>Procedimientos de Auditoria:</b> <ol style="list-style-type: none"> <li>1. Solicitar al área de recursos humanos de cada establecimiento de salud el curriculum vitae documentado de cada trabajador que administrará la base de datos de cada sistema de información.</li> <li>2. Comprobar los antecedentes consignados en el curriculum vitae como las certificaciones académicas y profesionales, comprobación de identificación.</li> <li>3. Verificar la firma del contrato de empleo, como también el documento firmado de confidencialidad y no divulgación de la información que se administrará.</li> </ol> | PT-01      |              |     |
|            |     |  | PT-02      |              |     |
|            |     |  | PT-03      |              |     |



|  |  |   |  |  |
|--|--|---|--|--|
|  |  | <p><b>Objetivo N° 2:</b></p> <p>Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.</p> <p>Criterio:</p> <ul style="list-style-type: none"> <li>- Reglamento de Organización y Funciones (ROF).</li> <li>- NTP - ISO / IEC 17799 - 2007</li> </ul> <p>Procedimientos de Auditoria:</p> <ol style="list-style-type: none"> <li>1. Solicitar el documento o guía donde está explícito la relación de responsabilidades asignadas a los trabajadores del área de estadística e informática según los roles de seguridad de información en cada establecimiento de salud. PT-04</li> <li>2. Verificar que el trabajador del área de estadística e informática ha recibido una inducción previa sobre el trabajo a realizar en los diferentes establecimientos de salud. PT-05</li> <li>3. Verificar si existe alguna documentación sobre el proceso formal disciplinario para empleados que han cometido alguna falta con respecto a la seguridad de la información. PT-06</li> </ol> <p><b>Objetivo N° 3:</b></p> <p>Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio,</p> |  |  |
|--|--|---|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  | <p>aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.</p> <p><b>Criterio:</b></p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 – 2008</li> <li>- ISO 22301:2012</li> </ul> <p><b>Procedimientos de Auditoria:</b></p> <ol style="list-style-type: none"> <li>1. Verificar si existe un plan de contingencia en la oficina de estadística e informática. PT-07</li> <li>2. Verificar si el plan de contingencia se ejecuta cuando es necesario. PT-08</li> <li>3. Solicitar el plan de pruebas. PT-09</li> </ol> <p><b>Objetivo N° 4:</b></p> <p>Verificar la prevención de pérdidas y daños en los activos, equipos e infraestructura adecuada, así como la interrupción de las actividades en el establecimiento de salud.</p> <p><b>Criterio:</b></p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 – 2008</li> <li>- POI de la DIRESA PIURA</li> </ul> <p><b>Procedimientos de auditoria:</b></p> <ol style="list-style-type: none"> <li>1. Verificar que la posición de los equipos minimicen el acceso innecesario a las áreas de trabajo, es decir que las personas no autorizadas tenga acceso. PT-10</li> <li>2. Verificar si los establecimientos de salud cuentan con alguna política de seguridad sobre la prohibición de fumar, beber y comer cerca de los equipos de PT-11</li> </ol> |  |  |
|--|--|--|--|--|

|  |  |   |       |  |  |
|--|--|---|-------|--|--|
|  |  | procesamiento de la información.  |       |  |  |
|  |  | 3. Verificar si la oficina de estadística e informática de los establecimientos de salud cuentan equipos y tecnología (software, cableado y servidores) adecuados para un funcionamiento continuo de los equipos que procesen todo tipo de información. | PT-12 |  |  |
|  |  | 4. Verificar que cuenten con generador de respaldo en funcionamiento cuando se prolongue la falta de energía eléctrica.   | PT-13 |  |  |
|  |  | 5. Verificar si cuentan con luces de emergencia y que se encuentren en funcionamiento.  | PT-14 |  |  |
|  |  | 6. Solicitar la documentación necesaria sobre la cantidad de fallos en los equipos, como las correcciones preventivas y correctivas, además de eso el periodo de tiempo en el que se realiza el mantenimiento a los equipos.                            | PT-15 |  |  |
|  |  | 7. Verificar antes de la baja de equipos los datos importantes y software con licencias.  | PT-16 |  |  |
|  |  | 8. Verificar si existe algún registro de autorización sobre la salida de equipos fuera de los establecimientos de salud.  | PT-17 |  |  |
|  |  | <b>Objetivo N° 5:</b><br>Verificar la operación correcta y segura de los recursos de procesamiento de información.<br>Criterio:<br>- NTP - ISO / IEC 17799 - 2007<br>- NTP - ISO / IEC 27001 – 2008   |       |  |  |

|  |  |   |   |  |  |
|--|--|---|---|--|--|
|  |  | <p>- <b>NORMAS DE CONTROL INTERNO</b></p> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Verificar si los digitadores tienen la documentación sobre los procedimientos de operación como por ejemplo los procedimientos de prendido y apagado, backups, mantenimiento de equipos, ambientes de cómputo y manipulación de correos.</li> <li>2. Verificar la existencia de documentación sobre procedimientos formales de gestión para asegurar un control de todos los cambios en los equipos y el software.</li> <li>3. Solicitar documentación sobre la segregación de funciones en el área de estadística e informática de los establecimientos de salud.</li> </ol> <p><b>Objetivo N° 6:</b></p> <p>Verificar el mantenimiento apropiado de la seguridad y recepción de la información en concordancia con los acuerdos tomados en la entrega de producción por parte del profesional de la salud.</p> <p><b>Criterio:</b></p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 - 2008</li> </ul> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Solicitar la documentación donde hace constar los plazos de entrega de información por parte de los profesionales de la salud.</li> </ol> | <p>PT-18</p> <p>PT-19</p> <p>PT-20</p> <p>PT-21</p> |  |  |
|--|--|---|---|--|--|

|  |  |   |       |  |  |
|--|--|---|-------|--|--|
|  |  | <p>2. Solicitar los informes de las auditorías realizadas a la información por las diferentes oficinas del nivel central.</p> <p><b>Objetivo N° 7:</b><br/>Verificar la integridad y disponibilidad del procesamiento de información y servicios de comunicación.</p> <p>Criterio:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 - 2008</li> </ul> <p>Procedimientos de auditoria:</p>   | PT-22 |  |  |
|  |  | <p>1. Solicitar las políticas de extracción de buckups de los sistemas de información, así mismo verificar que las copias de seguridad de la información estén guardadas en una locación remota, como por ejemplo discos extraíbles.</p> <p><b>Objetivo N° 8:</b><br/>Verificar que el acceso de usuario es autorizado de acuerdo a los perfiles de usuario de los sistemas de información</p> <p>Criterio:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 – 2008</li> <li>- Manual de organización y funciones(MOF)</li> </ul> <p>Procedimientos de auditoria:</p> | PT-23 |  |  |
|  |  | <p>1. Solicitar la documentación del control de acceso de cada usuario a los sistemas de información especificando además de los cambios, el pedido de acceso,</p>  | PT-24 |  |  |

Reg. 6359 - 12/10/15 LNP

|  |  |   |  |  |  |
|--|--|---|--|--|--|
|  |  | <p>autorización de acceso y administración de accesos.</p> <p><b>Objetivo N° 9:</b></p> <p>Verificar la existencia de perfiles de usuario en los sistemas de información.</p> <p>Criterio:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 – 2008</li> <li>- Manual de Organización y funciones (MOF)</li> </ul> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Solicitar la documentación de los perfiles de usuario de los sistemas de información.</li> <li>2. Solicitar la documentación de la asignación de contraseñas a los usuarios de los sistemas.</li> </ol> <p><b>Objetivo N° 10:</b></p> <p>Verificar que las debilidades en la seguridad de información asociados con los sistemas de información sean comunicadas de manera tal que permitan tomar acciones correctivas a tiempo.</p> <p>Criterios:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 27001 - 2008</li> </ul> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Solicitar el reporte de eventos sobre la pérdida de la seguridad de la información como por ejemplo fallas en los sistemas, errores humanos, pérdida de servicios o equipos.</li> </ol> | <p>PT-25</p> <p>PT-26</p> <p>PT-27</p> |  |  |
|--|--|---|--|--|--|

|  |   |       |  |  |
|--|---|-------|--|--|
|  | <p>2. Verificar el reporte inmediato de los eventos a una instancia superior por parte de los digitadores.</p> <p><b>Objetivo N° 11:</b><br/>Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.</p> <p>Criterios:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 – 2008</li> <li>- Normas de control interno</li> </ul> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Solicitar la planificación de las posibles auditorias por parte del encargado del área de informática.</li> <li>2. Solicitar todos los registros de auditoria ejecutadas a los sistemas por parte de un nivel superior.</li> <li>3. Verificar si existe el seguimiento de las recomendaciones dejadas en las supervisiones.</li> </ol> <p><b>Objetivo N° 12:</b><br/>Verificar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.</p> <p>Criterios:</p> <ul style="list-style-type: none"> <li>- NTP - ISO / IEC 17799 - 2007</li> <li>- NTP - ISO / IEC 27001 - 2008</li> </ul> <p>Procedimientos de auditoria:</p> <ol style="list-style-type: none"> <li>1. Verificar que los sistemas cumplan con</li> </ol> | PT-28 |  |  |
|  |   | PT-29 |  |  |
|  |   | PT-30 |  |  |
|  |   | PT-31 |  |  |
|  |   | PT-32 |  |  |

|  |  |   |  |  |  |
|--|--|---|--|--|--|
|  |  | <p>las políticas y estándares de seguridad de los establecimientos de salud.</p> <p><b>Objetivo N° 13:</b></p> <p>Verificar que la información almacenada en las bases de datos es de gran valor para la entidad, y esté protegida contra su pérdida o robo.</p> <p>Procedimientos de control:</p> <ol style="list-style-type: none"> <li>1. Solicitar las metas programadas en los años 2013, 2014 y 2015 de cada establecimiento de salud para evaluar su cumplimiento según la información.</li> <li>2. Verificar si existe algún incentivo o premio por cumplimiento de las metas programadas basadas en la información de casa sistema informático.</li> </ol> <p><b>Objetivo N° 14:</b></p> <p>Identificar las medidas de seguridad empleadas para conservar los datos correctos en la base de datos, con el fin de mantener su integridad.</p> <p>Procedimientos de control:</p> <ol style="list-style-type: none"> <li>1. Verificar que existen medidas de seguridad para conservar la integridad de los datos almacenados en cada sistema de información.</li> </ol> | <p>PT-33</p> <p>PT-34</p> <p>PT-35</p> |  |  |
|--|--|---|--|--|--|



Leyenda del programa detallado de auditoria:

- **NOMBRE:** se coloca las iniciales del nombre del especialista responsable del objetivo de control.
- **H/S:** son las horas por semana que se utilizarán para desarrollar cada procedimiento de control.
- **Ref. PT:** referencia al papel de trabajo que se usará para la ejecución del procedimiento de auditoria.
- **Hecho por:** se coloca las iniciales de los nombres de la persona que ejecuta los procedimientos de control.

#### **4.6.1.1 Formato para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: CURRICULOS VITAE**

**SR.  
JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el acceso a los currículos vitae de los trabajadores contratados del área de estadística e informática con la finalidad de dar cumplimiento al programa de auditoria y verificar los perfiles necesarios para el puesto que desempeña.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

## 4.6 Papeles de trabajo a aplicar

### 4.6.1 Papel de trabajo 01:

#### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-01

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

#### **Objetivo de Control:**

Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.

#### **Procedimiento:**

Realizar un documento dirigido al jefe de recursos humanos del establecimiento de salud solicitando los currículos vitae simples de los trabajadores para observarlos y comprobar que sus perfiles son los adecuados para el puesto en el que se está desempeñando.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

#### **Información Obtenida:**

- Currículos vitae.

#### **Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

#### **Anexos:**

- Solicitud dirigida al jefe de Recursos Humanos.
- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### 4.6.2 Papel de trabajo 02

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-02

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.

**Procedimiento:**

Mediante un documento dirigido al jefe de recursos humanos del establecimiento de salud solicitar los documentos que demuestren que se ha comprobado la experiencia profesional y las certificaciones académicas o verificar que están legalizadas.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Certificaciones de cada trabajador.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Solicitud dirigida al jefe de Recursos Humanos.
- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.2.1 Formato para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: OBSERVACION DE CURRICULOS VITAE**

**SR.  
JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar los documentos probatorios de la verificación de experiencia profesional y las certificaciones consignadas en los currículos vitae de los trabajadores contratados del área de estadística e informática, con la finalidad de dar cumplimiento al programa de auditoria y verificar los perfiles necesarios para el puesto que desempeña.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.3 Papel de trabajo 03

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-03

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que los trabajadores del área de estadística e informática cumplan con los requisitos indicados en el MOF de la institución.

**Procedimiento:**

Solicitar con documento al jefe de recursos humanos los contratos firmados de cada trabajador del área de estadística e informática, así como el documento firmado de confidencialidad y no divulgación de información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Contratos de cada trabajador.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Solicitud dirigida al jefe de Recursos Humanos.
- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.3.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: CONTRATOS DE TRABAJADORES**

**SR.  
JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar los contratos firmados por cada trabajador del área de informática y estadística, con la finalidad de verificar el vínculo laboral formal de cada trabajador y roles asignados.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

**“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL  
FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: DOCUMENTO DE  
CONFIDENCIALIDAD**

**SR.  
JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia del documento firmado de confidencialidad y no divulgación de la información de cada trabajador del área de informática y estadística, con la finalidad de verificar parte de la seguridad de la información.

Sin otro particular me despido de  
usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR



#### 4.6.4 Papel de trabajo 04

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-04

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.

**Procedimiento:**

Solicitar con documento al jefe de recursos humanos las funciones de cada persona que trabaja en el área de estadística e informática del establecimiento de salud.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documento de especificaciones de funciones.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Solicitud dirigida al jefe de Recursos Humanos.
- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.4.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: FUNCIONES DE TRABAJADORES**

**SR.  
JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar copia del documento en el que describe las funciones asignadas a cada trabajador del área de estadística e informática, con la finalidad de verificar el cumplimiento de la prevención de riesgos.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.5 Papel de trabajo 05

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-05

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.

**Procedimiento:**

Entrevistar a los trabajadores del área de estadística e informática para corroborar que han recibido algún tipo de inducción antes de empezar a laborar en esa área.

Luego, solicitar el Manual de Organización y Funciones para verificar si las funciones descritas anteriormente son correctas según el manual.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Manual de Organización y funciones.
- Entrevista a los trabajadores.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### 4.6.5.1 Formatos para el recojo de evidencias

##### ENTREVISTA N° 1

Fecha: ... de... de...

- ✓ Nombre del área en que labora:  
.....
- ✓ Fecha en que inicio labores en el centro de trabajo:  
.....
- ✓ Fecha en que recibió la inducción para iniciar labores de  
trabajo:.....
- ✓ Persona que brindo la enseñanza:  
.....
- ✓ Cargo que desempeña:  
.....
- ✓ Labores indicadas durante la inducción previa al inicio de trabajo:  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....
- ✓ ¿Quedó satisfecho con la enseñanza brindada?  
.....

---

AUDITOR

---

FIRMA DEL ENTREVISTADO

**“AÑO DE LA DIVERSIFICACIÓN PRODUCTIVA Y DEL  
FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: MANUAL DE  
ORGANIZACIÓN Y FUNCIONES**

**SR.**

**JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el manual de organización y funciones del establecimiento de salud, con la finalidad de verificar las funciones de los trabajadores del área de estadística e informática.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.6 Papel de trabajo 06

#### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-06

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

#### **Objetivo de Control:**

Verificar que todos los trabajadores del área de estadística e informática sean conscientes de los riesgos que afectan la seguridad de la información y que estén preparados para reducir el riesgo de error humano.

#### **Procedimiento:**

Solicitar al jefe de recursos humanos la documentación sobre las acciones que se deberán tomar en cuenta si existe alguna falta con respecto a la seguridad de la información.

Asimismo, solicitar si es que existe el record de faltas cometidas por el personal que labora en el área.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

#### **Información Obtenida:**

- Documentación sobre las acciones a las faltas cometidas.

#### **Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

#### **Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.6.1 Formato para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: NORMAS  
CORRECTIVAS FRENTE A UN  
ERROR EN LOS SISTEMAS.**

**SR.**

**JEFE DE RECURSOS HUMANOS DEL ESTABLECIMIENTO DE  
SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar la documentación sobre las normas correctivas cuando existe algún problema con respecto a la seguridad de la información.

Asimismo, solicito el registro del record de fallas cometidas por el personal que labora en el área de estadística e informática, con la finalidad de verificar la correcta gestión sobre la seguridad de la información de los sistemas de información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.7 Papel de Trabajo 07

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-07

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio, aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.

**Procedimiento:**

Solicitar con documento al jefe del área de estadística e informática el plan de contingencia de la oficina.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Plan de contingencia.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**



#### **4.6.7.1 Formato para recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PLAN DE  
CONTINGENCIA**

**SR.  
JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el plan de contingencia de la oficina de estadística e informática con la finalidad de constatar lo descrito en la NTP ISO 27001 – 2008.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.8 Papel de Trabajo 08

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-08

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio, aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.

**Procedimiento:**

Solicitar con documento al jefe del área de estadística e informática las medidas tomadas en base al plan de contingencia cuando existe algún tipo de inconveniente.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documentación sobre medidas basadas en el plan de contingencia.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.8.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: DESCRIPCION DE  
MEDIDAS APLICADAS BASADAS  
EN LA NTP ISO 27001-2008.**

**SR.  
JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar la descripción de las medidas tomadas frente a algún inconveniente con respecto a la seguridad de la información, las cuales están basadas en la NTP ISO 27001 – 2008.

Sin otro particular me despido de  
usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.9 Papel de trabajo 09

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-09

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Comprobar el diseño y la implantación de un plan de contingencia para garantizar a los usuarios la continua prestación del servicio, aún en circunstancias de emergencia en las que por problemas técnicos no se pueda prestar el servicio con la misma eficiencia que en circunstancias normales.

**Procedimiento:**

Solicitar con documento al jefe del área de estadística e informática las pruebas o plan de pruebas que la institución realiza para comprobar el plan de contingencia.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Plan de pruebas.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.9.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: PLAN DE PRUEBAS**

**SR.**

**JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo y a la vez solicitar el plan de pruebas que la institución usa para comprobar que el plan de contingencia es eficiente.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.10 Papel de trabajo 10

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-10

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Verificar que los equipos no estén al acceso de los pacientes ni que estos puedan observar los procesos durante el uso de equipos.

Además, verificar que las oficinas administrativas estén alejadas de los consultorios para atención con la finalidad de evitar contacto directo con los pacientes.

**Información Obtenida:**

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### 4.6.10.1 Formatos para el recojo de evidencias

- Fotos de los ambientes
- Fotos de la oficina de estadística e informática.

#### 4.6.11 Papel de trabajo 11

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-11

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

#### **Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

#### **Procedimiento:**

Solicitar al jefe del establecimiento de salud las políticas de seguridad con respecto a las prohibiciones de beber, fumar o comer cerca de los equipos de cómputo de la oficina de estadística e informática.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

#### **Información Obtenida:**

- Políticas de seguridad.

#### **Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

#### **Recomendaciones:**

#### **Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.11.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: POLITICAS DE  
SEGURIDAD.**

**SR.  
JEFE DEL ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo y a la vez solicitar haga extensiva las políticas de seguridad con respecto a las prohibiciones de fumar, beber o comer cerca de los equipos de cómputo de la oficina de estadística e informática del establecimiento de salud a su cargo.

Sin otro particular me despido de  
usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**



#### 4.6.12 Papel de trabajo 12

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-12

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos, equipos e infraestructura adecuada, así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Se aplicará una entrevista tipo checklist con preguntas referentes sobre el estado de la red, seguridad de red, estructura del sistema de cableado, data center, y medidas de prevención para riesgos que puede sufrir la red y equipos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Entrevista.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### 4.6.12.1 Formato para el recojo de evidencias

##### ENTREVISTA N° 02

- El área cuenta con topología UPS? Si es así ¿Cuál?
  - ☐ Standby
  - ☐ Línea iterativa
  - ☐ Standby – Ferro
  - ☐ On line de doble conversión
  - ☐ On line de conversión delta
- El área cuenta con un adecuado sistema de Control de HVAC:
  - ☐ Calefacción
  - ☐ Ventilación
  - ☐ Aire acondicionado
- Relacionados con el centro de datos, red y servidores:
  - ☐ Cuentan con sistema de puesta a tierra.
  - ☐ El centro de datos está en un área de muy poca concurrencia.
  - ☐ Cuentan con controles de acceso a la red
  - ☐ Cuentan con un sistema de puesta a tierra.
  - ☐ Tienen algún plan de seguridad física de red y centro de datos.
  - ☐ Cuentan con sistema de puesta a tierra.
  - ☐ Poseen un plan de mantenimiento de equipos y red
  - ☐ Posee un diagrama de distribución de red, data center y cableado.
- Referente al cableado:
  - ☐ Poseen cuarto de acometida (entrada de servicios)
  - ☐ Separan el cable UTP del coaxial y fibra óptica
  - ☐ Poseen sistema de canales de cable para evitar daños del mismo
- Método de conexión de equipos al centro de datos utilizada:
  - ☐ Conexión directa
  - ☐ Conexión cruzada
  - ☐ Cruzada
  - ☐ Conexión con fibra óptica

Entrevista realizada a: \_\_\_\_\_

Fecha: \_\_\_\_\_

\_\_\_\_\_  
AUDITOR

#### 4.6.13. Papel de trabajo 13

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-13

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Solicitar al jefe del establecimiento de salud realizar pruebas de cortes de fluido eléctrico para comprobar si el generador funciona.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Acta de verificación.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.13.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PRUEBAS CON EL  
GENERADOR DE ENERGIA.**

**SR.  
JEFE DEL ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar realizar las pruebas correspondientes a los cortes de fluido eléctrico para comprobar si el generador funciona.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.14 Papel de trabajo 14

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-14

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Solicitar al jefe del establecimiento permiso para realizar pruebas de funcionamiento de las luces de emergencia

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Acta de verificación.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.14.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PRUEBAS DE  
FUNCIONAMIENTO DE LAS  
LUCES DE EMERGENCIA.**

**SR.  
JEFE DEL ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar permiso para realizar pruebas de funcionamiento de las luces de emergencia del establecimiento de salud.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.15 Papel de trabajo 15

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-15

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

#### **Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

#### **Procedimiento:**

Solicitar al jefe del área de estadística e informática el registro de los fallos en los equipos, como las medidas tomadas en cada caso.

Además, solicitar el registro de fechas en que se realiza el mantenimiento de equipos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

#### **Información Obtenida:**

- Registro de fallos.
- Registro de fechas de mantenimiento de los equipos.

#### **Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

#### **Recomendaciones:**

#### **Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.15.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: REGISTRO DE  
FALLAS EN LOS EQUIPOS.**

**SR.**

**JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el registro y fecha en que los equipos de cómputo han fallado, así como las medidas que se aplicaron para revertir la situación dada.

Asimismo, solicito el registro de fechas en que se realiza mantenimiento a los equipos de cómputo.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**



#### 4.6.16 Papel de trabajo 16

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-16

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Solicitar al jefe del área de estadística e informática la descripción completa de equipos antes de proceder a la baja de los mismos por algún motivo específico.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Descripción de equipos antes de haberlos dado de baja.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.16.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: REGISTRO DE  
EQUIPOS.**

**SR.  
JEFE DE ESTADÍSTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el registro de equipos que se dieron de baja por diferentes motivos pertenecientes a la oficina de estadística e informática.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-17

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la prevención de pérdidas y daños en los activos así como la interrupción de las actividades en el establecimiento de salud.

**Procedimiento:**

Solicitar al encargado de logística el registro de salidas y devoluciones de los equipos que pertenecen a la institución.

Luego, solicitar alguna directiva en la que figure los tiempos límites de retorno de los equipos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documentos sobre el registro de salidas y devoluciones de equipos.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.17.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: REGISTRO DE  
SALIDA DE EQUIPOS.**

**SR.  
JEFE DE LOGISTICA DEL ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar el registro de equipos que solicitan para llevarlos fuera de la institución, así mismo cuando retornan a la institución.

Además, solicitar alguna directiva que demuestre los tiempos límites de retorno de cada equipo perteneciente a la institución.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-18

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la operación correcta y segura de los recursos de procesamiento de información.

**Procedimiento:**

Solicitar al jefe de estadística e informática la documentación de los procedimientos documentados como por ejemplo el registro de backups, procedimientos de prendido y apagado, mantenimiento de equipos y manipulación de correos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documentos sobre los procedimientos documentados.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.18.1 Formatos de recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: REGISTRO DE PROCEDIMIENTOS**

**SR.**

**JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar el registro de los procedimientos documentados como por ejemplo el registro de backups, procedimientos de prendido y apagado, mantenimiento de equipos y manipulación de correos.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.19 . Papel de trabajo 19

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-19

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la operación correcta y segura de los recursos de procesamiento de información.

**Procedimiento:**

Solicitar al jefe de estadística e informática del establecimiento de salud la documentación necesaria donde estén registrados el control de cambios en los equipos, en el sistema operativo, compras de licencias de los programas usados.

Verificar si los programas usados en las computadoras son originales.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documentos sobre el registro de control de cambios en los equipos.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria .
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.19.1 Formatos de recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: REGISTRO DE  
VARICIONES EN LOS EQUIPOS  
INFORMATICOS.**

**SR.  
JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar la documentación necesaria donde esté registrado el control de cambios en los equipos, en el sistema operativo, compras de licencias de los programas usados.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**



## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-20

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la operación correcta y segura de los recursos de procesamiento de información.

**Procedimiento:**

Realizar un documento solicitando al jefe de estadística e informática del establecimiento de salud la descripción de las funciones de cada trabajador en el área ya mencionada.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documentos sobre la descripción de funciones.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.20.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: DESCRIPCION DE  
FUNCIONES DEL PERSONAL.**

**SR.  
JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar la descripción de las funciones de cada trabajador en el área que tiene a su cargo, con la finalidad de verificar la distribución ordenada de las actividades que se realizan día a día.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-21

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el mantenimiento apropiado de la seguridad y recepción de la información en concordancia con los acuerdos tomados en la entrega de producción por parte del profesional de la salud.

**Procedimiento:**

Solicitar a la gerencia el acta donde constan los acuerdos tomados por parte de la oficina de estadística e informática y los profesionales de la salud con respecto a los tiempos prudentes de entrega de información para poder ingresarla a tiempo.

Verificar que la información ingresada sea en los tiempos establecidos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Actas de los tiempos establecidos para entrega de información.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.21.1 Formatos par el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

#### **SOLICITO: ACTA DE ACUERDOS TOMADOS**

**SR.  
JEFE DEL ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar copia del acta donde figura los acuerdos tomados por parte de la oficina de estadística e informática y los profesionales de la salud, con respecto a los tiempos prudentes de entrega de información con la finalidad de ingresar a tiempo y así mejorar la oportunidad de la información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-22

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el mantenimiento apropiado de la seguridad y recepción de la información en concordancia con los acuerdos tomados en la entrega de producción por parte del profesional de la salud.

**Procedimiento:**

Realizar un documento solicitando al jefe del área de estadística e informática copia de los informes de auditorías aplicadas a los sistemas de información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Actas de los tiempos establecidos para entrega de información.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.22.1 Formatos par el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: COPIA DE INFORMES  
DE AUDITORIAS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia de los informes de auditorías aplicadas a los sistemas de información que se ejecutaron hasta la fecha con la finalidad de verificar si las observaciones dadas se subsanaron.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud....

**Elaboró:**

**Referencia:** PT-23

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la integridad y disponibilidad del procesamiento de información y servicios de comunicación.

**Procedimiento:**

Solicitar al jefe de estadística e informática las políticas sobre la extracción de copias de seguridad de la información.

Verificar que las copias de seguridad estén guardadas en sitios seguros como por ejemplo discos extraíbles.

Solicitar el registro de fechas con respecto a las copias de seguridad de la información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Políticas de extracción de copias de seguridad de la información.
- Registro de fechas de extracción de copias de seguridad.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.23.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: POLITICAS SOBRE  
EXTRACCION DE COPIAS DE  
SEGURIDAD**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia de las políticas de extracción correspondientes a las copias de seguridad de la información de los sistemas, así mismo como las fechas en que se realizaron dichas copias de seguridad.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR



**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-24

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que el acceso de usuario es autorizado de acuerdo a los perfiles de los sistemas de información.

**Procedimiento:**

Solicitar al jefe de estadística e informática el documento pertinente sobre el control de acceso de cada digitador, especificando el usuario y contraseña a los diferentes sistemas de información, asimismo el módulo al que cada uno tendrá acceso en los sistemas.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documento de acceso para cada digitador.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.24.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: DOCUMENTO SOBRE  
CONTROL DE ACCESO DE  
USUARIOS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia del documento donde especifica el control de acceso de cada digitador, acotando el usuario y contraseña a los diferentes sistemas de información que se manejan en el área de estadística e informática como también el módulo que cada uno tendrá acceso en los sistemas.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-25

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la existencia de perfiles de usuarios en los sistemas de información.

**Procedimiento:**

Realizar un documento dirigido al jefe de estadística e informática solicitando los perfiles de usuario de cada sistema de información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documento de perfiles de usuarios.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.25.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PERFILES DE  
USUARIOS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia del documento donde especifica los perfiles de usuario en cada sistema de información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-26

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar la existencia de perfiles de usuarios en los sistemas de información.

**Procedimiento:**

Realizar un documento dirigido al jefe de estadística e informática solicitando la asignación de usuarios y contraseñas de cada persona que trabaja con cada sistema de información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Documento de asignación de usuarios y contraseñas.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.26.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: ASIGNACION DE  
USUARIOS Y CONTRASEÑAS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar copia del documento donde especifica la asignación de usuarios y contraseñas de cada persona que trabaja con cada sistema de información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-27

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que las debilidades en la seguridad de información asociados con los sistemas de información sean comunicadas de manera tal que permitan tomar acciones correctivas a tiempo.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática el reporte de fallas en los sistemas, la cantidad de errores humanos y la pérdida de equipos.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Reporte de fallas en los sistemas, cantidad de errores humanos y pérdida de equipos.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.27.1 Formato para el recojo de evidencia**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: REPORTES TECNICOS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar el reporte de fallas en los sistemas, la cantidad de errores humanos y la perdida de equipos.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR



## PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-28

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que las debilidades en la seguridad de información asociados con los sistemas de información sean comunicadas de manera tal que permitan tomar acciones correctivas a tiempo.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática los documentos necesarios donde figure el reporte inmediato de fallas en los sistemas, la cantidad de errores humanos y la pérdida de equipos a la gerencia para que se pueda tomar algún tipo de medida correctiva.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Informes a la gerencia.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.28.1 Formato de recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: INFORMES A LA  
JEFATURA**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar la documentación sobre los informes inmediatos que se envían a la jefatura, correspondiente a las fallas en los sistemas, la cantidad de errores humanos y la pérdida de equipos reportados.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

#### 4.6.29 Papel de trabajo 29

### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-29

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática la planificación por fechas de las posibles auditorías a ejecutar en el establecimiento de salud.

Verificar que esta documentación tenga la aprobación del jefe del establecimiento de salud.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Planificación de auditorías.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.29.1 Formato para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PLANIFICACION DE  
AUDITORIAS INTERNAS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar la documentación sobre la planificación por fechas de las posibles auditorías a ejecutar en el establecimiento de salud, con la finalidad de poder tener un control interno que indique las posibles mejoras en diferentes aspectos.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-30

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática las actas de supervisión del nivel central ejecutadas en el establecimiento de salud.

Verificar que existen informes realizados a la gerencia de las actas de supervisión para analizar como fue el proceso de auditoria ejecutada.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Actas de supervisión.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.30.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: ACTAS DE  
SUPERVISION**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL ESTABLECIMIENTO  
DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar la documentación sobre las actas de supervisión emitidas por el nivel central que se ejecutaron en el establecimiento de salud, así como los informes correspondientes a la jefatura sobre la supervisión dada.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.31 Papel de trabajo 31

#### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-31

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el cumplimiento de las recomendaciones derivadas de las auditorías realizadas a los sistemas de información.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática la documentación sobre el seguimiento de las recomendaciones de las auditorías ejecutadas a los sistemas de información.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Seguimiento de recomendaciones.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.31.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: ACTAS DE  
SUPERVISION**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar la documentación sobre el seguimiento de las recomendaciones producto de las auditorias ejecutadas a los sistemas de información tales como el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**



**PAPEL DE TRABAJO**

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-32

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática las políticas y estándares de seguridad de la información en el establecimiento de salud.

Verificar que los sistemas estén acorde con las políticas antes mencionadas.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Políticas y estándares de seguridad.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.32.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: ACTAS DE  
SUPERVISION**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar la documentación sobre las políticas y estándares de seguridad de la información en el establecimiento de salud.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

**AUDITOR**

PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-33

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que la información almacenada en las bases de datos es de gran valor para la entidad, y esté protegida contra su pérdida o robo.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática copia de las metas asignadas de los años 2013, 2014 y 2015 para evaluar si han cumplido con las metas programadas de acuerdo a la información generada en los sistemas.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Programación de metas.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.33.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: PROGRAMACION DE  
METAS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar copia de las metas programadas por la Dirección Regional de Salud durante los años 2013, 2014 y 2015 con la finalidad de evaluar el cumplimiento de las metas en base a la información generada por los sistemas de información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR

#### 4.6.34 Papel de trabajo 34

##### PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-34

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Verificar que la información almacenada en las bases de datos es de gran valor para la entidad, y esté protegida contra su pérdida o robo.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática copia de las resoluciones o algún tipo de incentivo por el cumplimiento de las metas programas por cada año.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Copias de resoluciones o fotos de otros tipos de incentivos.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.34.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: RESOLUCION POR  
CUMPLIMIENTO DE METAS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo cordialmente y a la vez solicitar copia de las resoluciones por cumplimiento de metas emitidas por la Dirección Regional de Salud o solicitar el permiso para la toma de fotografías de algún otro tipo de incentivos.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de,...

---

**AUDITOR**

PAPEL DE TRABAJO

**Unidad Administrativa:** Oficina de Estadística e Informática del establecimiento de salud...

**Elaboró:**

**Referencia:** PT-35

**Revisó:**

**Cédula:** Sistema de Información de Salud y el Aplicativo para el Registro de Formatos SIS.

**Objetivo de Control:**

Identificar las medidas de seguridad empleadas para conservar los datos correctos en la base de datos, con el fin de mantener su integridad.

**Procedimiento:**

Solicitar al encargado del área de estadística e informática las medidas de seguridad con respecto a la integridad de los datos que se almacenan en los sistemas de información en estudio.

Finalmente firmar el acta de recojo de información para iniciar la auditoria.

**Información Obtenida:**

- Medidas de seguridad con respecto a la integridad de los datos.

**Observaciones:**

**Situación:**

**Criterio:**

**Causa:**

**Efecto:**

**Conclusión:**

**Recomendaciones:**

**Anexos:**

- Acta de Apertura de Auditoria.
- Acta de Entrega de Documentos.

**Elaboró:**

**Fecha:**

**Supervisó:**

**Fecha:**

#### **4.6.35.1 Formatos para el recojo de evidencias**

### **“AÑO DE LA DIVERSIFICACION PRODUCTIVA Y DEL FORTALECIMIENTO DE LA EDUCACION”**

**SOLICITO: MEDIDAS DE  
SEGURIDAD DE LOS DATOS**

**A: JEFE DE ESTADISTICA E INFORMATICA DEL  
ESTABLECIMIENTO DE SALUD...**

Por el presente documento me dirijo a usted para saludarlo muy cordialmente y a la vez solicitar copia de las medidas de seguridad que se tienen en cuenta para verificar la integridad de los datos correspondientes a los sistemas de información.

Sin otro particular me despido de usted.

Atentamente;

Piura,... de..... de....

---

AUDITOR



## CONCLUSIONES

- En base al marco normativo peruano se desarrolló la propuesta del plan de auditoria informática que permite obtener una guía para las futuras auditorías a los sistemas informáticos del estado peruano (Aplicativo para el Registro de Formatos SIS y al Sistema de Información en Salud).
- Se ha identificado que la Guía para la implementación del Sistema de Control Interno de las entidades del estado emitida por la Contraloría General de la República establece que para poder establecer controles relacionados a las tecnologías de la información y comunicaciones debe tomarse en cuenta estándares o buenas prácticas internacionales, entre las cuales se encuentra la ISO/IEC 27001 que permita desarrollar un marco propio adaptable a la realidad de cada entidad perteneciente al sector público peruano. En ese sentido, considerando que la Contraloría General de la República no ha emitido normatividad explícita que permita guiar las auditorías de sistemas informáticos en entidades del sector público peruano, se hace necesario el uso de dichos estándares o buenas prácticas internacionales en las auditorías gubernamentales enfocadas a los sistemas informáticos, permitiendo de esta manera evaluar controles que podrían ser utilizados en los procesos informáticos de las entidades públicas con el fin de minimizar riesgos que puedan afectar el logro de los objetivos y metas institucionales.
- Se ha determinado que para poder hacer uso de la propuesta del plan de auditoria informática, se debe tener conocimiento de la normativa emitida por la Contraloría General de la República, Oficina Nacional de Gobierno Electrónico e Informática, estándares internacionales como la ISO/IEC 27001, así como normatividad propia emitida por la entidad que se está auditando, con el fin de tener una base adecuada que permita aplicar adecuadamente los temas abordados en la propuesta metodológica.
- Se ha determinado los documentos a aplicar en el plan de auditoria informática para que el auditor solo los aplique en la auditoria informática, es decir ya está listo el plan de auditoria informática para su ejecución netamente.

## **RECOMENDACIONES**

- El plan de auditoria informática propuesto en este trabajo de investigación debe ser considerado como un punto base para el inicio de auditorías en cada establecimiento de salud lo cual ayudaría a prevenir los riesgos informáticos que se presentan día a día.
- Capacitar al personal que labora en el área de estadística e informática con el tema ISO / NTP 27001: 2008 para que puedan tener conocimiento previo antes de iniciar la auditoria informática.
- Ejecutar auditoria internas en cada establecimiento de salud con la finalidad de tomar medidas correctivas en cuanto a la seguridad de los sistemas de información.
- Documentar procesos, roles y responsabilidades implicadas en la seguridad de la información, con el fin de hacer más sencillo el proceso de evaluación en futuras ocasiones y controlar así que las políticas y procesos de gestión de riesgos se estén cumpliendo.

## BIBLIOGRAFÍA

- ALFARO, E (2008). **Metodología para la auditoría integral de la gestión de la tecnología de Información**. Para optar el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú.
- ALIAGA, L (2013). **Diseño de un sistema de gestión de seguridad de información para un instituto educativo**. Para optar el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú.
- AUCANCELA, J (2012). **Auditoria de Riesgos Informáticos del Departamento de Sistemas de Caves SA EMA utilizando cobit como marco de referencia**. Para obtener el Título de Magister en Gerencia de Sistemas, de la Escuela Politécnica del Ejercito, Sangolqui.
- BALSECA, S Y CACHIMUEL, M (2008). **Evaluación y Auditoria Informática del Sistema de Información de la Escuela Politécnica del Ejército**. Para obtener el grado de Ingeniero de Sistemas, de la Escuela Politécnica del Ejército, Sangolquí.
- BARAHO NA, J Y GARZON, E (2014). **Auditoria de los riesgos informáticos en el departamento de tecnología de la empresa KUBIEC usando Cobit 4.1 y la norma ISO/IEC 27001 como marco de referencia**. Proyecto previo a la obtención del Título de Ingeniero en Sistemas Informáticos y de Computación, Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional, Quito Ecuador.
- CAJAMARCA, P (2013). **Auditoria de la gestión de las TIC'S para una empresa de aviación**. Proyecto previo a la obtención del Título de Ingeniero en Sistemas Informáticos y de Computación, Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional, Quito Ecuador.
- CARBAJAL, J. (2013); **Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano**. Tesis para la obtención de Master en Dirección Estratégica en Tecnologías de la Información, Facultad de Ingeniería de la Universidad de Piura.
- CORAISACA, J (2012). **Aplicación de Cobit 4.1 en la auditoria de una aplicación informática tipo web de una institución financiera**. Para optar el

Título de Ingeniero en Sistemas informáticos y de computación, Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional, Quito, Ecuador.

- CORONEL, K (2012). **Auditoria Informática orientada a los procesos críticos generados en la Cooperativa de Ahorro y Crédito “Fortuna” aplicando el marco de trabajo COBIT.** Tesis de grado previa a la obtención del Título de Ingeniería en Sistemas Informáticos y Computación de la Universidad Técnica Particular de Loja, Ecuador.
- GRANADOS, A (2012). **Auditoria del desarrollo de sistemas de información en el Gobierno Regional de Cajamarca.** Para obtener el grado de Ingeniero de Sistemas, de la Universidad Privada del Norte, Cajamarca.
- HUAMAN, F. (2014); **Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implementación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano.** Tesis para optar el título de Ingeniero Informático de la Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.
- MOLINA, J Y OÑA, D (2013). **Auditoria del sistema informático de la empresa “MANUFACTURAS AMERICANAS CIA.LTDA”.** Proyecto previo a la obtención del Título de Ingeniero en Sistemas Informáticos y de Computación, Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional, Quito Ecuador.
- PRADO, D (2009). **Metodología para el Establecimiento de Objetivos de Control como un medio de Seguridad en el Área de Tecnologías de Información.** Para obtener el grado de Maestro en Ciencias en Ingeniería de Sistemas, de la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional, México.

## ANEXOS

### 8.1 Anexo 01: Glosario

- **Atención preventiva:** Modelo de atención médica y de enfermería que se centra en la prevención de la enfermedad y en la conservación de la salud, y que consiste en el diagnóstico precoz de la enfermedad, el descubrimiento e identificación de las personas con riesgo de desarrollar problemas específicos, el asesoramiento y demás intervenciones necesarias para prevenir un problema de salud.
- **Atención recuperativa:** Es el modelo que consiste en brindar atención recurrente frente a una patología, y así poder ayudar a la población para la recuperación inmediata.
- **Equidad de salud:** significa que las personas puedan desarrollar su máximo potencial de salud independientemente de su posición social u otras circunstancias determinadas por factores sociales. La equidad en salud implica que los recursos sean asignados según la necesidad.
- **Emergencias:** situación crítica de peligro evidente para la vida del paciente y que requiere una actuación inmediata. Normalmente estamos frente a una emergencia cuando: La persona afectada está inconsciente, se sospecha que ha sufrido un infarto o tiene un paro cardíaco, hay una pérdida abundante de sangre, se sospecha que puede haber huesos rotos, se sospecha que puede haber heridas profundas, por ejemplo, de arma blanca, cuando se observan dificultades para respirar, cuando se observan quemaduras severas, cuando se observa una reacción alérgica severa, etc.
- **ISACA:** *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información).
- **Morbimortalidad:** son aquellas enfermedades causantes de la muerte en determinadas poblaciones, espacios y tiempos.
- **SIS:** Seguro Integral de Salud
- **Urgencias:** Es una situación de salud que se presenta repentinamente, pero sin riesgo de vida y puede requerir asistencia médica dentro de un período de tiempo razonable (dentro de las 2 o 3 horas).

## 8.2 Anexo 02: Consolidado de entrevistas a 10 Establecimientos de Salud

| RIESGO  | PREGUNTAS  | RESPUESTAS  |
|---|--|---|
| <b>Contratación de personal no calificado</b> | ¿El personal contratado ha entregado su currículo vitae documentado antes de iniciar sus labores?  | <ul style="list-style-type: none"> <li>- 6 establecimientos de salud respondieron que <b>NO</b> han entregado CV.</li> <li>- 4 establecimientos de salud respondieron que <b>SI</b> han entregado CV.</li> </ul>  |
|   | ¿Todos los trabajadores conocen el manejo del gestor de base de datos SQL SERVER?                  | - Los 10 establecimientos de salud manifestaron que todos los trabajadores <b>NO</b> conocen el manejo del gestor de base de datos.   |
|   | Tipo de profesión de los trabajadores de estadística e informática.                                | <ul style="list-style-type: none"> <li>- Asistentes sociales</li> <li>- Técnicos en computación</li> <li>- Ing. Industrial</li> <li>- Bach. Ingeniería Informática</li> <li>- Técnicos administrativos</li> </ul> |
| <b>Corte de fluido eléctrico</b>              | ¿Cuántas veces al mes en promedio el fluido eléctrico sufre cortes en el establecimiento de salud? | - En promedio 3 veces el fluido eléctrico sufre cortes según la entrevista aplicada a los 10 establecimientos de salud.   |
|   | ¿Posee la oficina de estadística e informática UPS?  | <ul style="list-style-type: none"> <li>- 9 establecimientos de salud manifiestan que <b>NO</b> poseen UPS</li> <li>- 1 establecimiento de salud <b>SI</b> tiene UPS.</li> </ul>                                   |

| RIESGO  | PREGUNTAS  | RESPUESTAS  |
|---|--|---|
| Falta de presupuesto por SIS o por recursos directamente recaudados | ¿La implementación de la oficina de estadística e informática se realiza en base a los recursos directamente recaudados (RDR) o por el ingreso del seguro integral de salud (SIS)? | <ul style="list-style-type: none"> <li>- 7 establecimientos de salud manifiestan que la implementación de la oficina es por RDR.</li> <li>- 1 establecimiento de salud manifiesta que la implementación es por RDR y por SIS.</li> <li>- 1 establecimiento de salud manifiesta que es por SIS.</li> <li>- 1 establecimiento manifiesta que no existe implementación.</li> </ul> |
| Exposición de equipos de cómputo al medio ambiente                  | ¿Los equipos están expuestos a los rayos solares? ¿Los equipos se malogran con frecuencia?   | <ul style="list-style-type: none"> <li>- 7 establecimientos de salud manifiestan que los equipos SI están expuestos al sol y que se malogran con frecuencia.</li> <li>- 3 establecimientos de salud manifiestan que los equipos NO están expuestos al sol ni se malogran con frecuencia.</li> </ul>   |
| Falta de internet   | ¿Poseen internet para las diferentes actividades que se realiza dentro de la oficina?  | <ul style="list-style-type: none"> <li>- 3 establecimientos de salud manifiestan que CASI SIEMPRE poseen internet.</li> <li>- 4 establecimientos de salud manifiestan que SI poseen internet.</li> <li>- 2 establecimientos de salud manifiestan que es LENTO el servicio de internet.</li> <li>- 1 establecimiento manifiesta que NO posee internet.</li> </ul>                |

| RIESGO                           | PREGUNTAS   | RESPUESTAS  |
|----------------------------------|---|---|
| <b>Falla en las aplicaciones</b> | ¿El sistema de información en salud o el aplicativo de registro de formatos SIS presentan errores frecuentes? | <ul style="list-style-type: none"> <li>- 9 establecimientos de salud manifiestan que <b>SI</b> existen errores en los sistemas de información.</li> <li>- 1 establecimiento de salud manifiesta que <b>NO</b> posee errores los sistemas de información.</li> </ul> |
|                                  | ¿Cada digitador tiene contraseña para el ingreso de la información?   | <ul style="list-style-type: none"> <li>- 5 establecimientos de salud manifiestan que cada digitador <b>NO</b> tienen contraseña.</li> <li>- 5 establecimientos de salud manifiestan que <b>SI</b> tienen cada uno su contraseña.</li> </ul>                         |

**Fuente: entrevistas a 10 establecimientos de salud de la unidad ejecutora 400**